

390

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

50023-146

U.S. APPLIC. NO. (if known, see 37 CFR 1.5)

09/914216

NATIONAL APPLICATION NO.

INTERNATIONAL FILING DATE

PRIORITY DATE CLAIMED

/P00/01097

FEBRUARY 25, 2000

FEBRUARY 26, 1999

FEBRUARY 26, 1999

E OF INVENTION

A MONITORING METHOD, DATA MONITORING DEVICE, COPYING DEVICE, AND STORAGE MEDIUM

PLICANT(S) FOR DO/EO/US

KIO KOJIMA, YASUHIRO KUWAHARA, AND TATSUMI WATANABE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendment has NOT expired.
 - d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information.
International Preliminary Examination Report
First Page of the Published International Application
International Search Report prepared by the Japanese Patent Office
Notification of Receipt of Record Copy



20277

PATENT TRADEMARK OFFICE

U.S. APPLICATION NO. (if known, see 37 CFR 1.50) <div style="font-size: 2em; font-weight: bold; margin-top: 10px;">09/914216</div>		INTERNATIONAL APPLICATION NO. PCT/JP00/01097		ATTORNEY'S DOCKET NUMBER 50023-146	
---	--	---	--	---------------------------------------	--

				CALCULATIONS	PTO USE ONLY
17. <input checked="" type="checkbox"/> The following fees are submitted: <div style="margin-left: 20px;"> Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO \$860.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) \$690.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) \$710.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$1,000.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$100.00 </div> <div style="text-align: right; margin-top: 10px;"> ENTER APPROPRIATE BASIC FEE AMOUNT = </div>					
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				\$ 00.00	
Claims	Number Filed	Number Extra	Rate		
Total Claims	37 -20 =	17	x \$18.00	\$ 306.00	
Independent Claims	11 -3 =	8	x \$80.00	\$ 640.00	
Multiple dependent claim(s) (if applicable)			+ \$270.00	\$ 00.00	
TOTAL OF ABOVE CALCULATIONS =				\$ 1,806.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				\$ 00.00	
SUBTOTAL =				\$ 1,806.00	
Processing fee of \$130.00 for furnishing the English translation later than the <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$ 00.00	
TOTAL NATIONAL FEE =				\$ 1,806.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property				\$ 40.00	
TOTAL FEES ENCLOSED =				\$ 1,846.00	
				Amount to be: refunded	\$
				charged	\$

a. ☐ A check in the amount of \$ _____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 500417 in the amount of \$ 1,846.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 500417. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

STEPHEN A. BECKER
 McDERMOTT, WILL & EMERY
 600 13th Street, N.W.
 Washington, DC 20005-3096
 (202) 756-8000
 Facsimile (202) 756-8087

SIGNATURE
STEPHEN A. BECKER
NAME
NO. 26, 527
REGISTRATION NUMBER
AUGUST 23, 2001
DATE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Akio KOJIMA, et al.

Serial No.:

Group Art Unit:

Filed: August 23, 2001

Examiner:

For: DATA MONITORING METHOD, DATA MONITORING DEVICE, COPYING
DEVICE AND STORAGE MEDIUM

09/914216

PRELIMINARY AMENDMENTCommissioner for Patents
Washington, DC 20231

Sir:

Prior to examination of the above-referenced application, please amend the application as follows:

IN THE DRAWINGS:

Please amend the Figures 2,9,10, and 12 as follows:

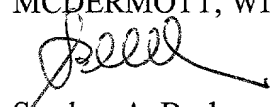
Please substitute the replacement Figures 2, 9, 10, and 12 with the Figures 2, 9,10, and 12 as originally filed.

REMARKS

Entry of this preliminary amendment is respectfully requested.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:ykg
Date: August 23, 2001
Facsimile: (202) 756-8087

09/914216

Fig. 9

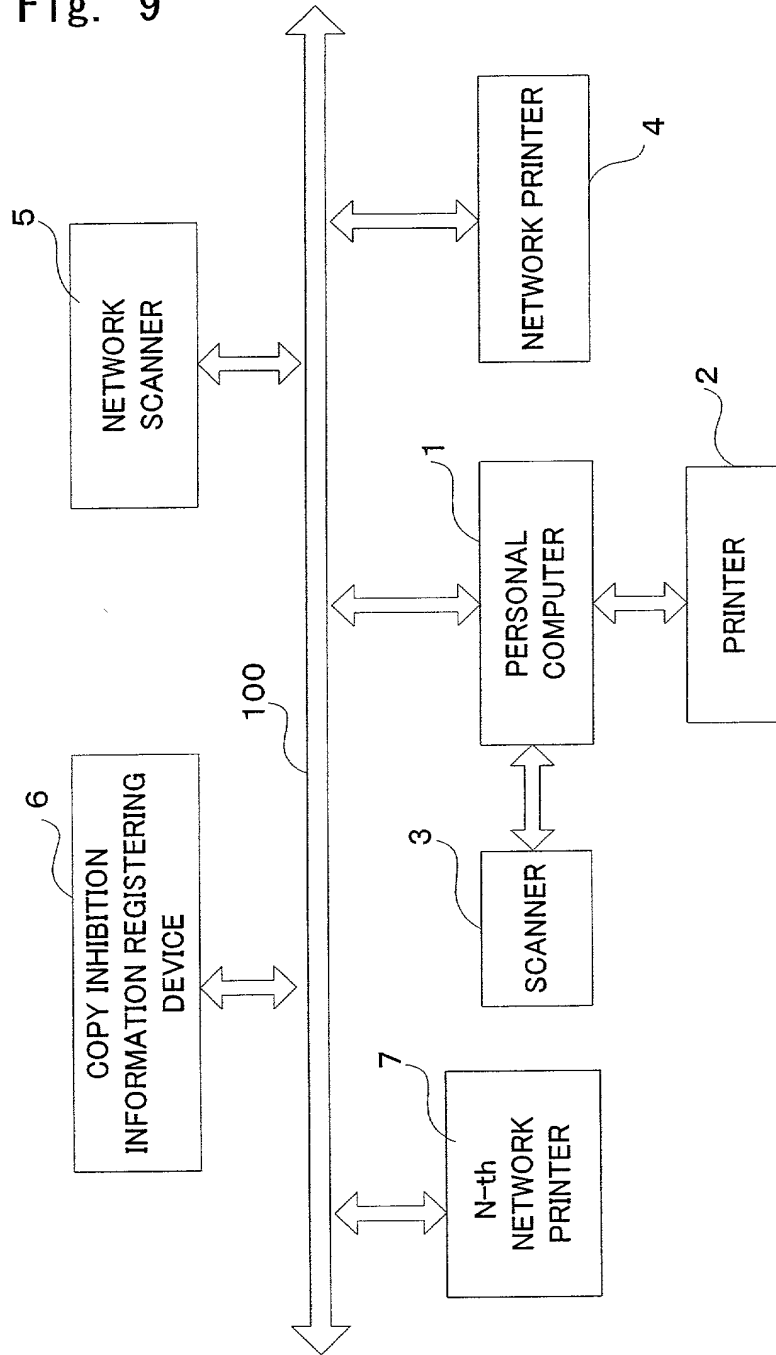


Fig. 10

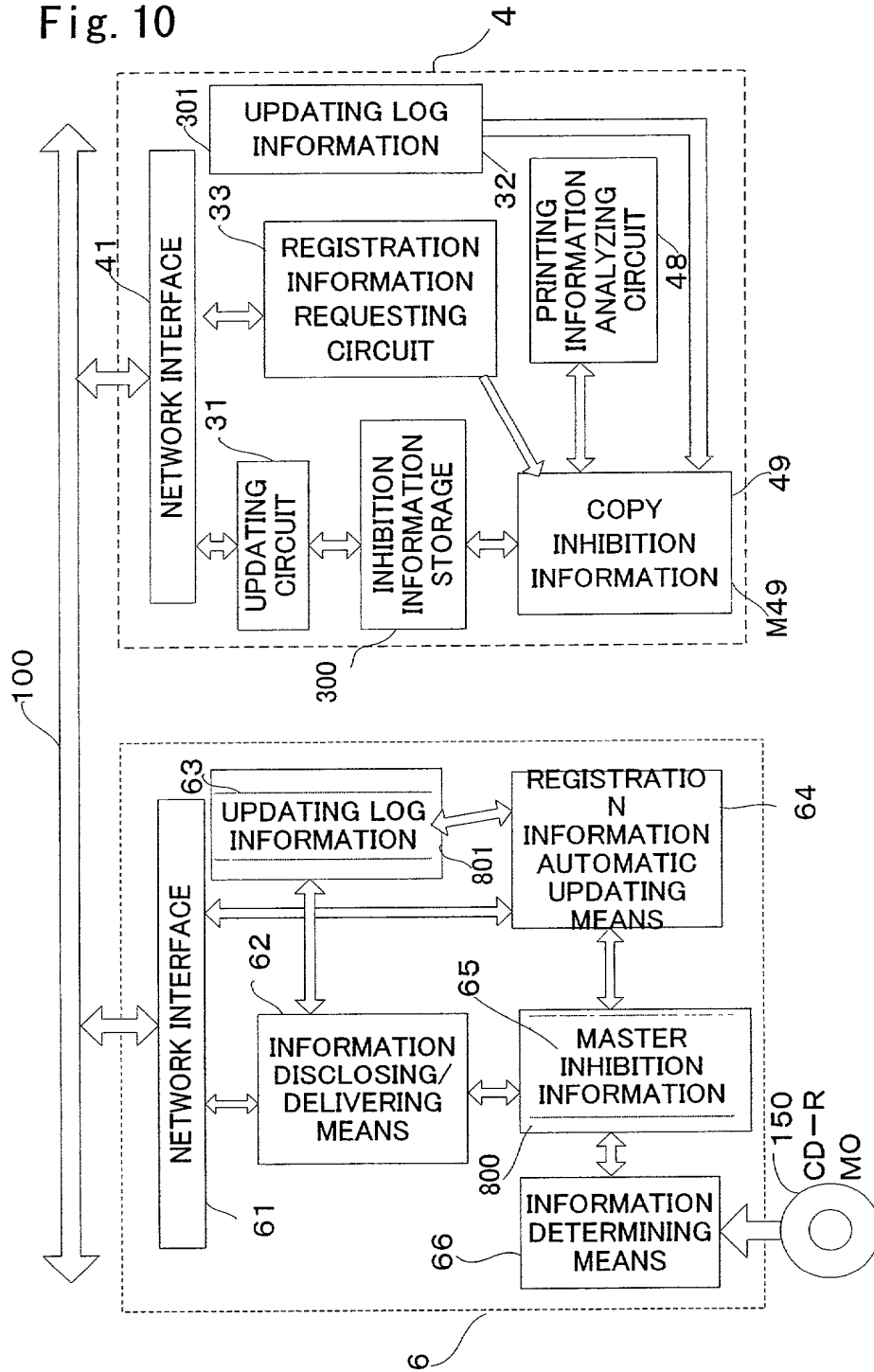
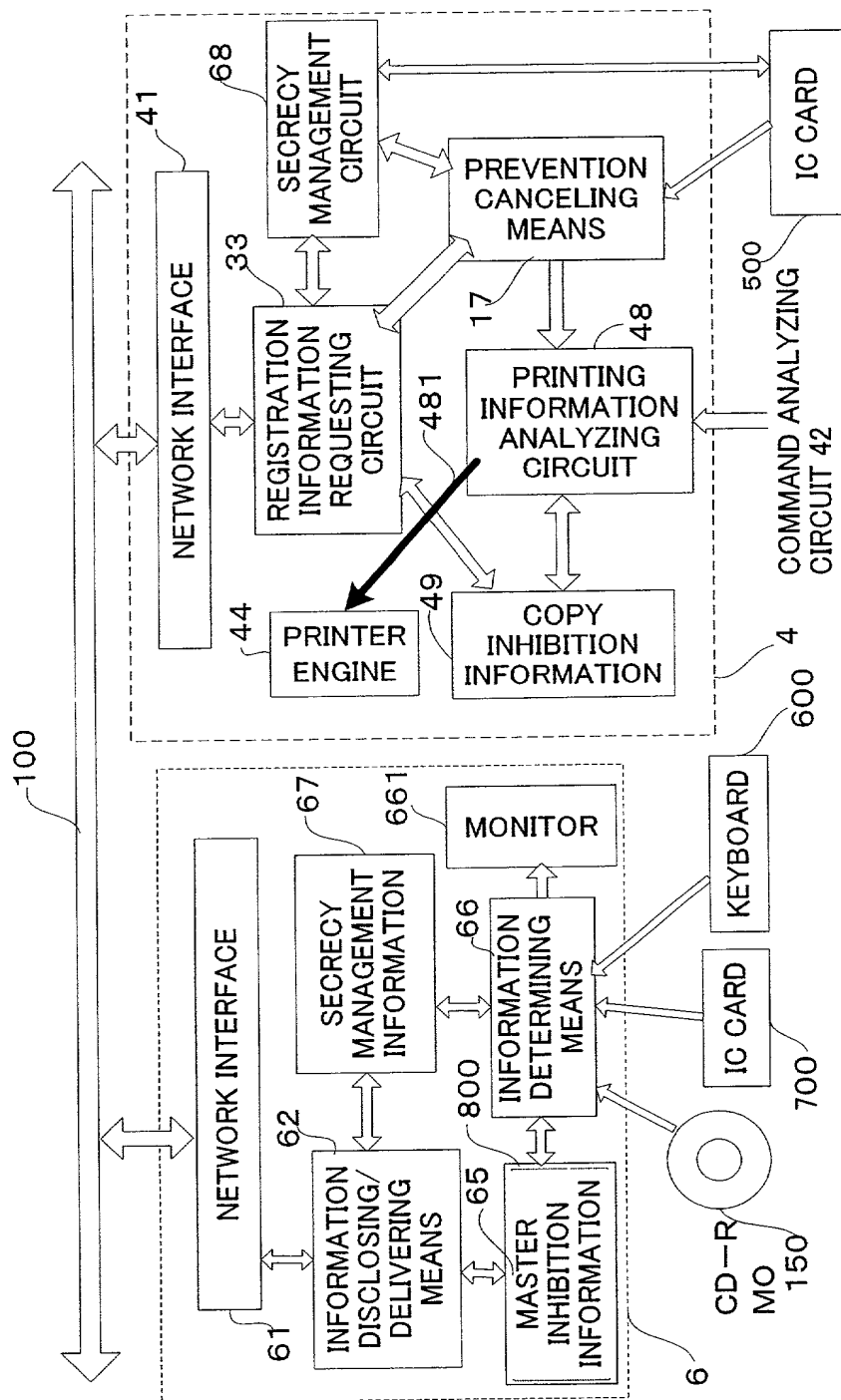


Fig. 12



18/PAT5

09/914216
JC05 Rec'd PCT/PTO 23 AUG 2001

Specification

DATA MONITORING METHOD, DATA MONITORING DEVICE,
COPYING DEVICE AND STORAGE MEDIUM

5 Field of the Invention

The invention relates to a data monitoring method for preventing copy-inhibited documents and image data from the unauthorized copying, and a device thereof.

10 Description of the Prior Arts

In these days, it has become easy for respective devices connected with the network to obtain and print electronic data, as the network and the digitalization develop wide. Meanwhile, the desktop Publishing (DTP), of which the technology has been improved in order to produce images close to
15 original data, can get copies more precise than ever. Thereby the infrastructure that enables a user to obtain electronic data and print them precisely is now consolidating.

On the other hand, the leak of secrecy regarding a document under the secrecy management gets into trouble in case where said
20 document is copied. In addition, if it is easy to obtain copies that cannot be distinguished from the original, it is afraid that such method is utilized to the illegal use of copyright or the forgery of bank notes and securities. The damages in such cases will be enormous.

The conventional color copying machine has installed the function
25 of preventing bank notes and etc. from the forgery. Fig. 18 shows a block diagram of the conventional color copying machine. In Fig. 18, image signals read from a scanner 110 are judged according to the image characteristics by

09914416.082301
"00000" 92447600

a specific image judging means 120 to be that of the bank notes and the securities being an object of the copying inhibition. In case of that of the copy inhibition, it is arranged that the copy prevention function be activated so that the images may be reproduced after the converting to a thumbnail
5 image or the reverse to a mirrored image. The image data thus processed in such a way may be outputted to a printer 130, so that the copied images can be easily distinguished as a forgery thing (for example, like an image processor disclosed in Japanese Laid-open Publication Nos. 01-316783, 11-275352, and 11-355562).

10 As the current trend, the number of documents and images, that are sent or received as paper documents or as electronic data, gets very large. There is a subject that a personal computer obtains secrecy electronic documents and copyright data in a simple way through network and then a high-speed printer copies the data illegally.

15 By the way, since the prescribed prior arts refers to the method for judging images of originals read by the scanner, it is not possible to deal with the prescribed subject regarding the electronic data that are not read by the scanner.

20 Besides, the prescribed prior arts have great influences over the society since it is very easy to forgery bank notes and etc., meanwhile it is possible only to inhibit the copying within the restricted limits. But, even in a specific business place, for example, there are various electronic data to be observed secret, and it is general that the contents of data are not constant for many hours but changeable along with the time elapsed.

25 However, it is hard for the prescribed prior arts to update the copy inhibition information at any time according to the environments.

Moreover, as electronic data gets to replace paper documents as

described above, the number of specific secrecy documents stored in a server has increased in the business place. In addition, it becomes possible for unspecified persons to display such secrecy documents on a display as a printed matter, and then to copy and browse the documents. There are
5 persons given an authorization to copy or browse these secrecy documents, while there are those not given. The restriction of the regulation varies depending on the kind of document. That is to say, there is a level of the secrecy management that is imparted to a document, and a specific person has to be allowed to copy and browse a document only when a management
10 level given to a specific person is higher than the management level included in the documents. However, even the conventional prior arts cannot administrate the copying and the browsing in due consideration of the secrecy management level of electronic data.

The present invention is suggested to settle the above problems,
15 and has an object to provide a data monitoring method and system that can prevent copy-inhibited data from the unauthorized copying beforehand and speedy.

The invention has another object to provide a data monitoring method and system that can freely update copy inhibition information
20 referring to the inhibition of the browsing and the copying according to the environment.

In addition, the present invention has the other object to provide a data monitoring method and system that can freely select either the allowance or the inhibition of the copying according to the secrecy
25 management level of electronic data.

Disclosure of invention

The invention adopts the following means in order to achieve the above objects. Specifically, monitoring means monitors each copy element of monitoring object data consisting of at least one kind of copy element in accordance with at least one kind of copy inhibition information capable of being updated and stored in inhibition information storage. Inhibiting means inhibits input or output of monitoring object data if the monitoring means determines that each copy element of the data agrees with a kind of the copy inhibition information. Therefore, it is possible to inhibit the copying and browsing of monitoring object data such as printing data and so on that agree with the copy inhibition information.

The above mentioned copy inhibition information can be updated by means of updating means. The updating is preferable to be executed by a user having a right to update. Additionally, the updating can be executed by obtaining new inhibition information from a removable storage medium or passing through the network.

On the assumption that the log of the updating of the copy inhibition information is stored in storage means, and it is arranged that, in updating the copy inhibition information, the updating be executed only when the updating information of the copy inhibition information is later than the stored log information.

On the assumption that secrecy management information corresponding to each copy inhibition information is stored in advance in inhibition information storage together with the copy inhibition information, and it is arranged that the copy inhibition and the inhibition cancel be controlled in accordance with the secrecy management information and the user's secrecy management level. Thereby, it is possible to inactivate the

function, if it is not necessary, to inhibit the copying and the browsing.

Since the copy inhibition information is concentrated and stored in a server device (master information storage) on the network, each device executing the copy inhibition processing can obtain the copy inhibition
5 information simply by accessing said server. In this case, the copy inhibition information may be transferred from the server device to each device passing through a removal storage medium, or may be transmitted via network. It is possible to store in the server device secrecy management information corresponding to each of copy inhibition information in addition to the copy
10 inhibition information.

The invention can inhibit the copying of printing data or browsing data as described above, and moreover can trace a device preparing a copied printed matter. That is to say, first specific information extracting means extracts ID information unique to a specific device concerned with the
15 preparation of monitoring object data, and information imparting means imparts the ID information to the monitoring object data, thereby new copied data is prepared.

The ID information may be chip ID information imparted to Central Processing Unit (CPU), an IP address imparted to a device, or the
20 like.

In addition, second specific information extracting means extracts specific application information unique to software concerned with the preparation of monitoring object data, and information imparting means imparts the specific application information to the monitoring object data,
25 thereby new copied data is prepared. It is effective that a mail address registered by a user is used as the specific application information.

A copying device, which receives monitoring object data from an

external device and prepares a copy based on the monitoring object data, can trace the copy as follows. That is to say, extracting means analyses the monitoring object data and extracts unique information specifying a specific device concerned with the preparation of the monitoring object data, and
5 then specific information imparting means imparts the extracted unique information to the monitoring object data.

It is helpful that ID number specifying a personal computer, or an IP address imparted to a device is used as the unique information.

Moreover, it may be arranged that extracting means analyze the
10 copied data and extracts unique information specifying software concerned with the copied data, and specific information imparting means imparts to a copy the extracted unique information as new copied data.

Brief Description of the Invention

15 Fig. 1 is a block diagram of a personal computer in the first embodiment of the invention.

Fig. 2 is a configuration diagram showing a system environment of a personal computer in the first embodiment of the invention.

20 Fig. 3 is a diagram showing copy inhibition information in the first embodiment of the invention.

Fig. 4 is a block diagram of a printing information analyzing circuit in the first embodiment of the invention.

Fig. 5 is a block diagram of a printer in the second embodiment of the invention.

25 Fig. 6 is a block diagram of a printing information analyzing circuit in the second embodiment of the invention.

Fig. 7 is a block diagram of a network scanner in the third

embodiment of the invention..

Fig. 8 is a block diagram of a network scanner in the fourth embodiment of the invention.

Fig. 9 is a diagram explaining a function registering on devices
5 connected with the network in the fifth embodiment of the invention.

Fig. 10 is a block diagram of a copy inhibition information registering device in the fifth embodiment of the invention.

Fig. 11 is an explanatory diagram of a prevention canceling circuit in the sixth embodiment of the invention.

Fig. 12 is a diagram showing the seventh embodiment of the
10 invention.

Fig. 13 is a diagram showing a table of the secrecy management information used in the seventh embodiment of the invention.

Fig. 14 is a block diagram of a personal computer of the eighth
15 embodiment of the invention.

Fig. 15 is a block diagram of a printer in the ninth embodiment of the invention.

Fig. 16 is a diagram showing a result of the printing in the ninth embodiment of the invention.

Fig. 17 is a block diagram showing a network printer in the tenth
20 embodiment of the invention.

Fig. 18 is a block diagram of a color copying machine of prior arts.

Preferred Embodiments of the Invention

25 The preferred embodiments of the invention are explained according to the drawings hereinafter. In addition, a term of the copying in the following explanation is defined as not only the case where a printed

matter equivalent to a specific data (an object data) is produced, but also a case where the object data is browsed by displaying the data on a displaying device. Accordingly, if the invention is applied to the browsing, the term including "print" ("printing data", for example) should be change to "browse" ("browsing data"). In order to distinguish a working memory from a nonvolatile storage medium such as a hard disk, the reference numeral M is imparted to a working memory.

(Embodiment 1)

Fig. 1 is a block diagram showing the first embodiment of the invention. Fig. 2 is a block diagram showing a configuration of the system environment of a personal computer. Fig. 3 is a diagram showing an example of inhibition information described hereafter. And Fig. 4 is a block diagram showing in detail a part shown in Fig. 1.

When a simple printing system is configured in a personal computer 1 (which will be described as PC 1 hereafter) by installing various applications as shown in Fig. 2, it is possible for the PC 1 to perform the editing and the image processing (color processing). When a scanner 3 is selected as inputting means, image data is read by the scanner and then imputed in the PC 1. A printer 2 as copying means produces a printing image on a recording paper, an OHP paper or the like in accordance with the printing data of the PC 1.

When the PC 1 is connected with a network 100, the image data may be read by a network scanner 5, and the printing data may be transferred to a network printer 4 and printed thereby.

The DTP system comprises the scanner 3 for inputting an object original to the PC1 as described above, the PC1 for the color or other processing of images read by the scanner, and the printer 2 for printing the

image. In addition, it is needless to say that the object image may be graphics data prepared by an application installed in the PC1 instead of the images read by the scanner.

Next, the operation that the PC1 prints specific printing data 11 is explained here referring to Fig. 1.

Fig. 1 is a functional block diagram in case where the PC1 works under a specific printing application. The image data, which is inputted from outside through the scanner and etc. or prepared inside of the PC1 by an application for the image preparing, is stored as a printing data 11 in a printing information memory M11. Under these conditions, when a user selects the printing, the printing data 11 is sent to a printer driver 12. At this time, since the printing information memory M11 is predetermined to be a working memory, there are some cases that the printing data 11 stored in advance in a hard disk is given to the working memory, the printing data 11 inputted from the scanner is given direct to the working memory, or the like.

The printer driver 12 has been previously installed as a control program for handing data from the PC 1 to the printer 2. The printer driver 12 transfers to the printer 2 the printing data 11 selected to be printed by the application.

In Fig. 1, data monitoring means comprises printing information analyzing circuit 15 and an inhibition information memory M14 storing copy inhibition information 14. Besides, the inhibition information memory M14 is given on demand copy inhibition information from inhibition information storage 300 that will be described later. The copy inhibition information 14 may be anything that can specify the printing information aiming at every printing matter such as documents, bank bills, securities, and cash vouchers. The kind of the copy inhibition information is not restricted to one kind, but

there are various kinds as described later. And the inhibition information memory M14 are a working memory like the printing information memory M11.

The printing data 11 is given to the printer 2 from the printer driver 12, and also given to the printing information analyzing circuit 15 composing the data monitoring means 400. The printing information analyzing circuit 15 expands on a confirmation memory M16 copy elements, such as character string information described in the metalanguage, image pattern information, code information, and encryption information embedded by the digital watermark method of the printing data 11 to be transferred to the printer 2. The expansion in this stage does not mean that of bitmap data, but that of data in a form printable by a printer. For instance, the copy elements may be expanded to the intermediate language like a displaying list, or to the state of ASCII code of characters. Besides, the code information means a specific pattern corresponding to a code (a number, a mark, and so on) that is decoded to the number or the code by the code analyzing engine described later.

Moreover, the printing information analyzing circuit 15 collates and analyzes the copy elements of the expanded printing data 11 with the copy inhibition information 14 stored in the inhibition information memory M14 (which will be described later in detail). When determining that the copy element of the printing data 11 agrees with one of the copy inhibition information 14 previously stored in the inhibition information memory M14, the printing information analyzing circuit 15 outputs a stop order 151 to the printer driver 12 in order to stop transmitting the printing data. According to the stop order 151, inhibiting means 121 provided with the printer driver 12 stops transmitting the printing data to the printer 2.

Therefore, the above method can prevent the unauthorized copying in the step that the printing data passes through PC 1.

It is arranged in the invention that the contents of the copy inhibition information 14 can be updated corresponding to the contents to be inhibited from the printing. Thereby, the invention can accommodate to the secrecy management level and the secrecy information that are updated day by day, and also to the forgery preventing technology and the encrypting technology of which the technology development is rapidly advancing.

That is to say, while information updating circuit 13 including functions of updating means and obtaining means has registered in advance an ID of person having a right to update, an IC card 200 registers the same ID representing the person having the right to update. Under this condition, it is arranged that the information updating circuit 13 may authenticate the IC card 200 when the IC card 200 is inserted into card reading means of the PC 1.

At this time, if it is authenticated that the person having a right to update is going to update, the copy inhibition information 14 obtains updating data stored in the IC card 200 and is updated from the contents previously stored in the inhibition information storage 300 such as a hard disk to that data (there is a case where contents are written in newly).

Besides, the updating of the IC card 200 itself is executed by a sever device (a copy inhibition information registering device 6 shown in Fig. 12, for example) storing information to be a master of the copy inhibition information 14 (master inhibition information) and a separated PC working the server device or the like. At the time of updating the IC card 200, the date (or the version of the updated contents) is registered in the IC card as the updating log. On the other hand, when the contents of the inhibition

information storage 300 is updated according to the IC card, the date (or the version of the updated contents) is also registered in the inhibition information storage 300. And then it is preferable that the information updating circuit 13 updates the contents of the inhibition information storage 300 when the date of the IC card is later than that of the inhibition information storage 300. Thereby, it is possible to avoid the unnecessary updating (see the fifth embodiment).

It is needless to say that the updating data may be obtained passing through the network 100. That is to say, a server device (the copy inhibition information registering device 6 shown in Fig. 11, for example) for storing master inhibition information to be original information of the copy inhibition information 14 should be provided on the network. Under this arrangement, the information updating circuit 13 accesses to the server device on the network on demand or at fixed periods and then obtains the master inhibition information from the server device (see the fifth embodiment).

Besides, even when the copy inhibition information is obtained through the network as described above, it is preferable that the inhibition information storage 300 may store only the latest information by comparing the data or the like of the updating of the original information on the server device with the date or the like of the latest updating of the copy inhibition information stored in the inhibition information storage 300.

Moreover, by presetting IDs of persons having a right to update in the server device, it is arranged that an instructor of the updating is judged to be an authorized person or not according to each individual ID sent via network. That is to say, the information updating circuit 13 transfers the information for the updating-right registered in the IC card to the server

device together with the user ID, when a person without the right requests the updating, the master inhibition information (copy inhibition information) is not transmitted to the PC side. However, unlike the above case, the copy inhibition information is not necessary to be written into the IC card used
5 here.

Since the invention includes the function of updating as described the above, it is possible to perform the updating of copy inhibition information easily, and to maintain that the contents be the latest edition. In addition, since there is no necessity for changing a built-in memory (ROM),
10 the updating can be performed quickly and it is possible to prevent the spread of the unauthorized copying.

Moreover, by performing the authentication of a person with the updating-right, it is possible to guard the data from persons making the unauthorized copying or the illegal change.

15 The copy inhibition information 14 obtained as above are stored in the inhibition information memory M14 from the inhibition information storage means 300 at the time of copying, which is shown in Fig. 3.

A field F141 of the inhibition information memory M14 stores character information 141 such as a title in a document, specific character strings in a document (for example, a significant keyword of a confidential document or the like), and etc. A field F142 stores image pattern information
20 unique to and specifying the printing information. For instance, when a specific pattern (or a character string) is corresponding to a specific code, the association information between the pattern (or the character string) and the
25 code are stored.

In addition, A field F144 stores encryption information 144 like decryption information of digital watermark embedded in photo image data

protected by the copyright, and decryption algorithm of encryption pattern and type information of code, which are previously printed on originals to be read by a scanner 3 according to a specific encryption (security printing, etc.).

It is possible to accommodate these copy inhibition information 14
5 to every document and every original by adding with necessary information. Additionally, the copy inhibition information 14 is also able to apply to a case where a displaying device is used as outputting means instead of the printer.

For instance, when the data monitoring method of the invention is applied to the displaying system using a display like CRT and so on, it is
10 enough that specific figures, codes or the like embedded in still images or moving images to be inhibited from the browsing (copy) may be added as new copy inhibition information to each prescribed one.

Next, it is arranged as shown in Fig. 4 that printing information analyzing circuit 15 always monitors the printer driver 12 and never fails to
15 work specific operations before starting the printing.

First, when the printing information analyzing circuit 15 starts the operation, a drawing engine 154 acquires copy elements composing the printing data 11 from the printer driver 12 and draws each copy element into a confirmation memory M16. In this way, each copy element 161 drawn into
20 the confirmation memory M16 is analyzed in its content by each analyzing engine.

That is to say, out of copy elements 161 of object data (printing data 11) expanded on the confirmation memory 16, title data is extracted by a title analyzing engine 155, and the result of the analyzed contents is
25 transmitted to a collating circuit 159. The collating circuit 159 selects character information 141 usable as collation information out of copy inhibition information 14 stored in the inhibition information memory M14,

which are collated with analyzed result transmitted from the title analyzing engine 155. In a result of the collating, if agreeable information is found, it is considered that the unauthorized copying is executed; thereby the stop order makes the printer drive 12 stop the printing.

5 There are many methods for extracting titles by the title analyzing engine, however, the title analyzing engine regards and extracts regions gathering large sized characters in the object data as a title in general.

10 Likewise, a document analyzing engine 156 extracts text data from copy elements expanded on the confirmation memory M16, and then transmits said data to the collating circuit 159. And an image analyzing circuit 157 extracts a part of photo from the copy elements expanded on the confirmation memory M16, and then transmits said data to the collating circuit 159. In addition, a code analyzing circuit 158 extracts specific codes
15 (numerical values, symbols) by decoding the copy elements expanded on the confirmation memory M16, and then transmits said data to the collating circuit 159.

20 The collating circuit 159 selects character (text) information 141, image pattern information 142, code information 143, and encryption information 144, such data usable as the collating information, out of the copy inhibition information 14 respectively. And respective information is collated with the analyzed result transmitted from each analyzing engine. In a result of collating, when the printing information that agree with any one of the copy inhibition information is found, it is consider the unauthorized
25 printing, thereby the stop order 151 makes the printer driver 12 stops the printing.

 In the steps of the above collating, the collating circuit 159 in

response to inquiries from each analyzing engine may acquire necessary information out of the copy inhibition information 14 and response to each analyzing engine. For instance, the code analyzing engine 158 requires decoding algorithm and the key at the time of decoding. For that reason, the
5 code analyzing engine 158 asks the collating circuit 159 about the decoding algorithm necessary for the decoding, and then obtains the latest decoding algorithm from the inhibition memory M14. Thereby the code can be decoded. When a specific code is converted to regular information, it is necessary for the association of the code and the corresponding regular information. In this
10 case, the collating circuit 159 obtains the association from the inhibition memory 14, and then gives said data to the code analyzing engine 158.

As described above, the invention can accommodate to the printing originals with various kinds of characteristics by a plurality of analyzing engines.

15 In addition, the invention can be made more effective by providing the data monitoring device of the invention with a secrecy management function.

The secrecy management function through network will be described in the seventh embodiment. Here is described regarding the
20 secrecy management function executed by the data monitoring device.

That is to say, secrecy management information 67 indicating a secrecy management level has been imparted to each copy inhibition information as shown in Fig. 13, for example (the explanation about Fig. 13 will be made in the seventh embodiment). On the other hand, the secrecy
25 management level has been imparted to a user of the PC 1 together with the user ID, of which content was registered in an IC card 500, for example. Under these conditions, when a user uses the PC 1, the user makes a secrecy

management circuit 68 read the IC card 500. The secrecy management circuit 68 sends the readout content to prevention canceling means 17. When the copy elements of the printing data 11 are expanded on the confirmation memory M16 as described above, the prevention canceling means 17 judges if the user has a right to copy and browse the copy elements, referring to the secrecy management information 67 of copy elements being analyzed by the printing information analyzing circuit 15. As the result, if the user is judged to have a right to copy and browse, the inhibition processing of the printing information analyzing circuit 15 is canceled.

Therefore, it is possible to prevent the printing information analyzing circuit 15 from working even in case where there is no need to inhibit the copying or the browsing.

Beside, the IC card 500 may be common to an IC card registering the right of updating, however, it is preferable that the right of updating may be treated as the data different from the secrecy management level. It is needless to say that the secrecy management processing can be applied to a printer and a scanner that are described as follows.

In the first embodiment as described the above, since the PC 1 is provided with the function of preventing the unauthorized copying by analyzing the printing contents when the PC1 instructs the printer to print out, it is possible to previously prevent the unauthorized copying of secrecy documents in companies, and the forgery of bank bills and cash vouchers. In addition, since the invention is provided with a configuration that can update the copy inhibition information in easy, the invention can cope with the secrecy management level and the secrecy information that are changed day by day, and the technologies of the forgery prevention and the encryption that progress rapidly. Consequently, it is possible to prevent the spread of

the unauthorized copying.

Moreover, it is possible to prevent any person from changing information or performing the unauthorized copying by authenticating and confirming if the person has a right to update. And since the management
5 level can be imparted, the management of the secrecy information can be carried out in various levels.

Furthermore, when the preventing function of the unauthorized printing is provided to the personal computer, there is no need for any special hardware, but to install software only. Therefore, it is possible to cut
10 cost.

(Embodiment 2)

The first embodiment refers to a case where the personal computer is provided with the preventing function of the unauthorized copying, meanwhile the following explanation will describe the embodiment
15 wherein a printer is provided with the preventing function of the unauthorized copying.

The operations of a printer 2 will be explained referring to Fig. 2 and Fig. 5. Fig. 5 is a block diagram of the printer 2.

A receiving buffer of the printer 21 receives printing data from the
20 PC 1, and the printing data is transmitted to a command analyzing circuit 22 one after another. The command analyzing circuit 22 analyses the language and the image data format of the received printing data. Next, in a result that the command analyzing circuit 22 performs the analyzing, if it is necessary for drawing characters and graphics, the printing data is sent to a
25 graphics/character drawing circuit 23. The graphics/character drawing circuit 23 draws the specific graphics and characters on an image memory M26 via memory controller 25. Likewise, in a result that the command

analyzing circuit 22 performs the analyzing, if it is necessary for expanding photo data, the printing data is sent to an image drawing circuit 27. The image drawing circuit 27 expands the specific photo data on an image memory M26 via memory controller 25. When the expansion of the desired image data is formed on the image memory M26, the memory controller 25 transmits the image data to a printer engine 24. The printer engine 24 prints on recording papers according to the received image data.

In Fig. 5, the data monitoring means 400 comprises an inhibition information memory M29 including a printing information analyzing circuit 28 and copy inhibition information 29.

The printing information analyzing circuit 28 composing the data monitoring means 400 monitors image data expanded on the image memory M26 as mentioned above, and analyses the contents of the image data before the image data is transmitted to the printer engine 24. If the contents of the image data agree with the information stored in the inhibition information memory M29, a stop order 218 is outputted. When receiving the stop order 218, inhibiting means 241 provided in the printer engine 24 stops the operation of the printer engine 24.

Next, the function of an updating circuit 30, since that as the updating means is almost same as that explained in the first embodiment, will be explained hereafter regarding the different points from that of the first embodiment. Besides, the inhibition information memory M14 and the information updating circuit 13 in the first embodiment are corresponding to a inhibition information memory M29 and a information updating circuit 30 respectively. Although the inhibition information storage 300 may be a hard disk, it may be preferable to be a rewritable nonvolatile memory with small capacity like a flash memory because there is not so much large size of data

to be stored in the printer.

The steps of the updating by the IC card 200 are same as that in the first embodiment. And the updating data may be obtained from the PC 1. At any time, at the fixed period, at the unfixed period, or at the time of the printing, the PC 1 transmits to the printer 2 the updating data together with the printing data. The updating data is received by the command analyzing circuit 22 passing through the receiving buffer 21. At this time, the command analyzing circuit 22 detects updating data 221 from the order codes defined aside from the printing data, and transmits the updating data 221 to a updating circuit 30.

The updating data obtained from the PC 1 may be either one of that the PC 1 received passing through the network 100, or that the PC 1 received from a removable recoding medium. In this case, the confirmation of the update-right should be performed by the PC 1 side.

Besides, the contents of the copy inhibition information 29 used in this embodiment is quite same as that of the copy inhibition information 14 explained in the first embodiment, of which explanation will be omitted here.

Next, a printing information analyzing circuit 28 shown in Fig. 6 is almost same as the printing information analyzing circuit 15 shown in Fig.

4. The processing within the PC 1 needs to expand the printing data sent from the printer driver 12 on the confirmation memory M16 by the drawing engine 154 as described in the first embodiment, on the other hand, it is arranged in this embodiment that the printing data transmitted from the PC 1 be expanded on the image memory M26.

As described above, the processing after the step of expanding the printing data is same as that of the first embodiment except that the reference numerals of circuits differ respectively.

The effect based on the above configuration is also same as that in case where the invention is applied to the prescribed PC, however, the moving picture cannot be regulated by the copy inhibition. Merely, it is possible to activate each prescribed engine whenever each frame of moving picture is printed out by the printer.

(Embodiment 3)

The second embodiment refers a case where the data monitoring function should be installed into the printer to prevent the unauthorized copying, meanwhile the followings will explain the embodiment where the data monitoring function is installed to a scanner.

The operation of a network scanner 5 will be explained according to Fig. 7. Fig. 7 is a block diagram of the network scanner 5.

An original being an object (not shown) is read by an image sensor 51, which is converted to digital image data by an A/D converter 52. The image data is transmitted toward the network passing through a network interface 54 (which will be described as a network I/F 54 hereinafter) after the image processing like the edge emphasizing to emphasize edges of characters in the image or the color processing by image processing circuit 53.

The data monitoring means 400 comprises inhibition information memory M56 including an inputting information analyzing circuit 55 and copy inhibition information 56. The inputting information analyzing circuit 55 composing the data monitoring means 400 judges if the original is inhibited from the printing according to the information stored in the copy inhibition information 56. When it is detected that the original is inhibited one, a stop order 551 is outputted to the network I/F 54. At receiving the stop order 551, inhibiting means 541 provided in the network I/F 54 stops the

output of the image data.

The copy inhibition information 56 stored in the inhibition information memory M56 is the same as the copy inhibition information 14 shown in Fig. 3, of which explanation is omitted here. Besides, the copy inhibition information 56 can be updated by an information updating circuit 57 in the same steps described in the first or the second embodiment. The updating steps by the information updating circuit 57, as explained in the first or the second embodiment, may obtain the updating information form other devices connected with network passing through the network I/F 54, otherwise can obtain the updating information from a removable IC card 200 or a memory card. Besides, as described in the second embodiment, a hard disk may be used as the inhibition information storage 300, but it may be preferable to use a rewritable nonvolatile memory with small capacity like a flash-memory because there is not so much large size of data to be stored in the network scanner.

However, this embodiment is considered from a case where the copy inhibition information is obtained directly from a server (master information storage means) on the network without using a hard disk or a flash-memory.

The scanner 5 is provided with a registration information requesting circuit 58 (information obtaining means), on the other hand, the network is provided with a server device (the copy inhibition information registering device 6 shown in Fig. 10, for example) that stores original information of the copy inhibition information 56 (which has the same contents as the copy inhibition information 56) as explained in the fifth embodiment. Thereby, the copy inhibition information 56 can be obtained via network by the registration information requesting circuit 58. Therefore,

since it is not necessary for installing a memory for storing huge information,
it is possible to reduce the cost of the products.

It is supposed that the server device on the network is set up
either one of the specific business places. In this case, it is arranged that the
5 inputting information analyzing circuit 55 activates the registration
information requesting circuit 58 automatically at the time of reading
originals and then accesses to the server device to obtain the necessary copy
inhibition information 56. The copy inhibition information 56 is stored
directly in the inhibition information memory M56 that is a working memory
10 in the network scanner instead of storing a hard disk or the like, wherein the
data is provided to the comparing and the collating of the inputting
information analyzing circuit 55.

It is needless to say that the registration information requesting
circuit 58 can be adapted to the personal computer in the first embodiment,
15 or the printer in the second embodiment.

Besides, it is a matter of course that the scanner of this
embodiment is applied to not only a scanner connected with the PC 1 via
network but also a scanner connected direct with the PC 1.

As described in the above third embodiment, the network scanner
20 5 does not need to install a memory to store huge information because the
registration information requesting circuit 58 can obtain the same contents
as the copy inhibition information 56 via network. Therefore, the invention is
useful for any device that is not usually provided with a hard disk, such as a
printer, a scanner, or the like.

25 The device provided with the inhibition information storage 300
updates the contents of the inhibition information storage 300 according to
the information obtained from the IC memory 200 or via network, of which

the effect is the same as that of the first and the second embodiment, therefore the explanation will be omitted here.

(Embodiment 4)

The third embodiment refers to a case where the data monitoring
5 function is installed into a scanner; meanwhile this embodiment explains a case where a network printer comprises the data monitoring function.

Fig. 8 is a block diagram of a network printer 4.

The network printer 4 receives printing data from a device connected with the network. A command analyzing circuit 42 receives the
10 printing data and sends the instruction command via network interface 41 (which is called a network I/F 41 hereunder), and analyses the language and the image data format of the received printing data. In addition, the command analyzing circuit 42, a graphics/characters drawing circuit 43, an image drawing circuit 47, and a memory controller 45, of which reference
15 numerals differ from that of the printer explained in the second embodiment but the functions are the same, are not explained here.

When desired image data is formed on an image memory M46, the memory controller 45 transmits the image data to the printer engine 44. The printer engine 44 prints on recording papers the image data in the order of
20 receipt.

A printing information analyzing circuit 48 composing the data monitoring means 400 (the printing information analyzing circuit 48 and a copy inhibition information memory M49) monitors printing data interpreted by the command analyzing circuit 42, and analyses the contents of the image
25 data before transmitting said data from the image memory M46 to the printer engine 44. If the contents of the image data agree with any one of the copy inhibition information 49 stored in the copy inhibition information

memory M49, a stop order 481 is outputted. At receiving the stop order 481, the inhibiting means 441 provided in the printer engine stops the operation of the printer engine 44. It is needless to say that, like the second embodiment, the printing information analyzing circuit 48 may monitor and
5 analyze the image memory M46.

Next, like the updating circuits 30, 31, or 57 in each prescribed embodiment, an updating circuit 31 can update the content of the copy inhibition information stored in the inhibition information storage 300 corresponding to the content to be inhibited. The kind and the steps of the
10 updating methods of this copy inhibition information 49 are not explained here because those are the same as the explanation in each prescribed embodiment. Besides, since the network printer is a device to be connected with the network, it is useful to update the copy inhibition information via network 100 like the third embodiment.

15 (Embodiment 5)

The first to the fourth embodiments explain about devices in which the data monitoring function is installed, on the other hand, this embodiment explains about one example of the method for delivering quickly the copy inhibition information to a device comprising the data monitoring
20 function. That is to say, it is arranged that the PC, the scanner, and the printer described in each prescribed embodiments are to receive the delivery of the copy inhibition information concentrated on the sever device (the copy inhibition information registering device), thereby the copy inhibition information can be in common use among devices.

25 According to Fig. 9 and Fig. 10, the registration function of the copy inhibition information will be described. Fig. 9 is a diagram explaining the registration function on a device connected with the network. Fig. 10 is a

block diagram of a copy inhibition information registering device.

In order to prevent the unauthorized copying, an important thing is how speedy the copied data being an object can be detected and be prevented from the copying. The copy inhibition information registering device 6 shown in Fig. 9 is a device delivering via network the copy inhibition information to the network scanner 5, the network printer 4, the personal computer 1, and the n-th network printer 7; those devices connected with the network.

In the preventing function of the unauthorized copying that is installed in each device, updating means installed in each device (updating means 13, 30, 31, or 57) obtains updating data from the copy inhibition information registering device 6, and then updates the contents of the copy inhibition information to the latest edition. Therefore, it is possible to deliver the information about the unauthorized copying to each device in speedy without bearing the user's load, and to prevent the unauthorized copy in advance.

The copy inhibition information registering device 6 is explained in detail according to Fig. 10. Fig. 10 is a block diagram of the copy inhibition information registering device.

In Fig. 10, information determining means 66 obtains master inhibition information 65, which are originals of copy inhibition information, from a recoding medium such as a floppy disk or CD-ROM.

The method of inputting the master information into the information determining means 66 is to input directly from a keyboard or input image patterns from a scanner, except the usage of the above-mentioned removable storage medium. The information determining means 66 obtaining the master inhibition information as above writes the

master inhibition information 65 into the master inhibition information storage 800. If the master inhibition information has already written into the master inhibition information storage, the contents are written over.

Another method of updating the master inhibition information 65 is executed passing through the network 100. In this case, it is necessary to arrange in advance that registration information automatic updating means 64 may obtain updating data from a designated database. When the registration information automatic updating means 64 receives the updating data, the updating log information 63 (for example, the updating date or the version of the updating contents) is stored in the log storage 801. Thereby, the registration information automatic updating means 64 can judge whether it is necessary to update the master inhibition information 65 or not, comparing the updating date of the database on the network and the updating date of its self. The registration information automatic updating means 64 may execute the updating at regular time intervals, otherwise may execute the updating according to the notification from the database. The master inhibition information storage means 800 and the log storage 801 are sufficient to use different areas in a same hard disk respectively.

Information disclosing/delivering means 62 transfers as the copy inhibition registration information the master inhibition information 65 stored in the master inhibition information storage 800 in response to a request via network 100 (see the third embodiment). Additionally, in response to updating requests from updating circuits 13, 31 or 57 of devices controlled by the copy inhibition information registering device 6, such as a printer, a scanner, or a personal computer, the master inhibition information 65 is delivered to the updating circuits as the copy inhibition registration information.

information analyzing circuit 48, and then obtains the master inhibition information 65 stored in the master inhibition information storage 800 direct from the information disclosing/delivering means 62, and even may store the data in the inhibition information memory M49.

5 Therefore, since the network printer side does not need a memory for storing the copy inhibition information 49, it is possible to reduce the cost. In addition, since the copy inhibition information 49 of the network printer 4 can be updated by updating the master inhibition information 65, it is easy to control the management and it is possible to accommodate to the updating
10 quickly.

 Since the updating logs executed by the updating circuit 31 are stored in the inhibition information storage 300 as the updating log information 32, it is possible to avoid that the registration information requesting circuit 33 may issue any invalid request.

15 In the fifth embodiment as described above, the copy inhibition information registering device 6 can disclose/deliver the master inhibition information 65 toward each device connected with the network, it is easy to perform the maintenance and the management of devices and change levels of the secrecy information.

20 Moreover, by changing information of one device, the information of all the devices controlled on the network can be updated at one time; therefore it is possible to prevent the unauthorized copy speedy.

 The above explanation refers to the delivery via network only, however, even when the copy inhibition information centralized in a point
25 delivers to each device by a removable recoding medium such as an IC card (for example, the IC card 200 of the first embodiment), copy inhibition information device 6 can fulfils its satisfactory function.

(Embodiment 6)

Fig. 11 is a block diagram showing an embodiment of a method canceling the unauthorized copy preventing function of a device comprising the data monitoring function.

5 For the maintenance of the device, or for some reason or others, there is a need for canceling the unauthorized copy preventing function. A user having a right to cancel the function inserts into a prevention canceling circuit 17 an IC card 201 that can executes the canceling. The prevention canceling circuit 17 authenticates the IC card 201 and then instructs the
10 printing information analyzing circuit 15 (28, 55) to stop its function. Thereby, it is possible to stop the function preventing the unauthorized copy.

Otherwise, it may be arranged to stop the function of the printing information analyzing circuit 15 (28, 55), when a specific password is inputted from the network or a specific key of the decryption is inputted from
15 a keyboard.

At all events, the canceling method may be a way of specifying a user having a right to cancel the function. Since the prevention canceling circuit 17 comprises a function for registering data of the authentication, such as the number of the IC card 201 and etc., from the keyboard or the
20 network, thereby the authentication of the IC card 201 can be performed. Therefore, it is possible to accommodate to various management conditions like the change of organization, the moving of apparatuses, the change of the secrecy levels or the like.

In the sixth embodiment as mentioned above, it is possible to
25 perform the maintenance of devcies by utilizing the prevention canceling circuit 17. Additionally, the prevention canceling circuit 17 has a function of registering the number of the IC card and etc.; thereby it is possible to carry

out the flexible management.

In the first to the sixth embodiments as described as above, it is possible to prevent the unauthorized copy speedy.

(Embodiment 7)

5 A method that a printer comprising the data monitoring function manages secrecy information via network will be described in this embodiment according to Fig. 12 and Fig. 13. Fig. 12 is a diagram explaining the management of secrecy information, and Fig. 13 is a diagram explaining the contents of the management information.

10 In Fig. 12, the master information storage 800 of the copy inhibition information registering device 6 is provided with secrecy management information 67 in addition to the master inhibition information 65; thereby, it is possible for the management of secrecy information to accommodate to the updating of the managed information, the limitation of
15 allowing to display or to print for a person who accesses to the data in speedy.

 Here is explained about the method of managing the secrecy information. As described in the sixth embodiment, the master inhibition information is stored in a removable recoding medium or in the master
20 information storage 800 via network.

 Under the above arrangement, a specific administrator inserts an IC card 700 to the copy inhibition information registering device 6 in order to inform that he has a right to update. Information determining means 66 of the copy inhibition information registering device 6 reads the contents of the
25 IC card 700, and confirm whether the user has a right to update or not. If the user has a right to update, the secrecy management information 67 inputted from a keyboard 600 by using a monitor 661 is accepted.

The information determining means 66 is to write into the a table 670 shown in Fig. 13, for example, the secrecy management information 67 thus inputted together with the master inhibition information 65. That is to say, in the table 670 an information ID is for specifying the master inhibition information (copy inhibition information), a permit level explains a secrecy level represented by alphabet and numbers; each alphabet indicates the secrecy level raising in the alphabetical order and respective numerals following to the alphabet indicates the secrecy level raising in the order of numbers. And the group ID indicates a control department of the master inhibition information, and an individual ID is for identifying a user. Therefore, for instance, regarding the master inhibition information (copy inhibition information) D001, the output of the information will be allowed for a user having a permit level over the A001 and included in X00. And it is defined that the copying and the browsing are allowed for the user having the individual ID of ID1/PW1 in addition to the above conditions.

The secrecy management information 67 thus inputted is referred by secrecy management circuit 68 on the printer 4 side. Specifically, a user inserts an IC card 500 into the secrecy management circuit 68 before using the printer 4. The secrecy management circuit 68 reads the contents of the IC card 500 and stores the secrecy management level registered in the IC card such as the permit level, the group ID, and the individual ID together with the user ID.

Next, when receiving specific printing data from the PC and so on and expanding said data on the image memory M46 (see Fig. 8), as described in the fifth embodiment the registration information requesting circuit 33 obtains the copy inhibition information 65 via network interface 41 and stores said data in the inhibition information memory M49 while obtaining

the corresponding secrecy management information 67 from the table 670 and sending the data to inhibition canceling means 17. The inhibition canceling means 17 compares the secrecy management level 67 corresponding to the copy elements in the printing information analyzing circuit 48 being an object of the collating and the secrecy management level of the user stored in the secrecy management circuit 68. When the secrecy management of the user is higher than that of the secrecy management information 67, the printing information analyzing circuit sends to a printer engine 44 a signal 481 that the user is an allowable person; thereby the desired printing matter can be obtained.

If the user is an unallowable person, the instruction of the canceling is not sent to the prevention canceling means 17 meanwhile the inhibition of printing the specific information is set. With reference to the copy inhibition information 49, the printing information analyzing circuit 48 issues the signal 481 for specifying the inhibition object and then stops the printer engine 44.

As mentioned above, it is possible to accommodate speedy to the updating day by day since a device comprises the function registering the management information of secrecy information. Additionally, it is possible to carry out the precise control of the copying and the browsing in association with the registering device of the secrecy information by providing the secrecy management function with the printer 4. It is also possible to carry out the detailed configuration of the information disclosing operation, like the level controlling of the copying and the browsing per each title group according to the permit level, per position or organization according to the group ID, or per specific person according to the individual ID. When the registering device is provided on the network, if there is any change of

organization or change of layout, it is possible to carry out the secrecy management speedy. It is better that managing items, such as device information to be inhibited from output, the information of the management period, and etc., are arranged to be extendable at any time.

5 Besides, the method of the individual authentication may adopt the recognition of a fingerprint of hand, a face, or a retina of eye instead of the IC card 500, any method of which can specify an individual can be applied to this invention.

10 Moreover, the invention is explained taking the printer as an example, however, it is possible to prevent the undesired disclosing of the secrecy information by providing the data monitoring function of the invention with a displaying device and adding the secrecy information management function to each device.

15 Furthermore, the invention can be applied to a displaying device of every portable intelligent terminal such as a Personal Digital Assistance (PDA), a mobile phone, a notebook-type computer and etc. without limiting to a displaying device of a specific personal computer.

20 Furthermore, the invention can be also applied to an audio outputting device (a speaker). Though it is not shown practically, when device information to be inhibited is added to the audio outputting device as the secrecy management information 67, it is possible to perform the inhibition control to the outputting media like the displaying of the image information is allowed but the audio information is inhibited to output.

25 At all events, it is possible to control the disclosing level of every device and terminal connected with a network by providing the management function of the secrecy information with each device.

 The first to the sixth embodiments as described as above explain

regarding a case where the copying is inhibited by using the copy inhibition information. However, the following eighth to tenth embodiments explain a configuration that is able to specify and trace a device when unauthorized copies are outputted by a personal computer, a printer, a scanner or the like.

5 (Embodiment 8)

Fig. 14 is a block diagram of an information imparting circuit for imparting ID information, which is unique to a device, to printing data to be printed by a printer.

An information imparting circuit 18 extracts CPU ID information
10 18a included in a central processing unit (which is called CPU hereunder) installed the PC 1, and sends the information to a printer driver 19. The printer driver 19 imparts the CPU ID information 18a to printing data 11 stored in a printing memory M11, which is outputted as new printing data to a printer 2. In this case, since the CPU ID information 18a is proper and
15 unique to the PC 1, the ID is effective as information resource for managing users.

Likewise, the information imparting circuit 18 obtains from each application software 92 application registration information 18b provided with the PC, and sends the information to the printer driver 19. The
20 information to be registered is time information and information of user who uses a device, like the user registration information and mail address. The printer driver 19 imparts the application registration information 18b to the printing data 11, which is sent to the printer 2 as a new printing data.

The application registration information 18b is user information
25 at the installing, a specific product No. assigned to user, a user password, and etc. The mail address set in an application by a user is valid to trace an address of the operating user and becomes an information resource valid to

specify a device, a location, and the time of user concerned with the copying. The registration information of the operating system (which is called OS hereafter) of the PC 1 may be used as the application registration information 18b. The application registration information may be substituted with any information of the installed software that can specify a user or software.

Likewise, the information imparting circuit 18 extracts hardware information 18c installed in the PC 1, and then sends the information to the printer driver 19. The printer driver 19 imparts the hardware information 18c to the printing data 11, which is outputted to the printer 2 as a new printing data. The information imparting circuit 18 obtains as hardware information the information of a substrate installing the CPU of the PC 1 and IP address configured in the network interface 93. Information of the connected printer 2 may be obtained from a driver.

In the 8th embodiment as described above, the information for specifying the location, the time and the operating user of the device or the software can be detected automatically and then imparted to the printing data, thereby it is possible to trace the location, the time and the operating user that the copies originated from. Therefore since a device outputting the copies can be detected quickly and the preparation status of the printing data remains as the evidence, it is possible to suppress the spreading of the unauthorized copying and minimize the leak of the secrecy information.

(Embodiment 9)

Fig. 15 is a block diagram of a printer provided with a tracing function.

The printer 2 receives the printing data from the PC 1 by making use of the receiving buffer 21, and sends the printing data to the command

analyzing circuit 22 one after another. The command analyzing circuit 22 analyses the language and image data format of the received printing data.

While analyzing the language and image data format of the received printing data, the command analyzing circuit 22 extracts ID
5 information 222 (the device information, the software information, the hardware information) to be imparted to the printing data automatically, and then send the data to a specific information imparting circuit 80.

Next, according to a result analyzed by the command analyzing circuit 22 as described above like the first embodiment, the
10 graphics/character drawing circuit 23 executes the drawing of characters and graphics on the image memory M26, meanwhile the image drawing circuit 27 expands photo data on the image memory M26.

In addition, the specific information imparting circuit 80 modulates the ID information 222 at specific pattern on the image memory
15 M26 via the memory controller 25, and then imparts the data to the image expanded on the image memory M26. For example, the specific information code 1000 is imparted on the printing data 261 as shown in Fig. 16, otherwise may be sent direct to the printer engine 24 a specific pattern, which is printed on a recording paper.

20 When a desired image data is formed on the image memory M26, the memory controller 25 transfers the image data to printer engine 24. The printer engine 24 performs the printing based on the received image data.

In the 9th embodiment as described above, the printer 2 extracts the imparted specific information from received printing data, and then
25 imparts the specific information to the printing data automatically when the printer 2 prints the printing data in its self. Thereby it is possible to trace a device that performs the unauthorized copy of confidential documents in

company or the forgery of bank notes and cash vouchers.

(Embodiment 10)

Fig. 17 is a block diagram of a printer connected with the network and provided with the tracing function.

5 The printer 4 receives printing data from the PC 1 via network interface 41, and then sends the printing data to a command analyzing circuit 42 one after another. The command analyzing circuit 42 analyses the language and the image data format of the received printing data.

10 Next, a graphics/character drawing circuit 43 draws characters and graphics, and an image drawing circuit 47 expands photo data; since these processing are the same as in the first to the eighth embodiment, the explanations are not described here.

15 The specific information imparting circuit 80 extracts from the network interface 41 an IP address 223 imparted to the printer 4, and modulates the IP address 223 at specific pattern on an image memory M46 via a memory controller 45, and then imparts the data to the expanded image. The imparted form is the same as in the 9th embodiment and the IP address is imparted on the printing data as the specific information code as shown in Fig. 16. It is needless to say that this IP address may be extracted
20 from the command analyzing circuit 42 as described in the 9th embodiment. And it is may be arranged that the IP address be sent direct to the printer engine 44 as a specific pattern and printed on a recording paper.

25 When the desired image is formed on the image memory M46, the memory controller 45 transfers the image data to a printer engine 44. The printer engine 44 performs the printing based on the received image data.

 In the 10th embodiment as described above, the ID information (IP address) of the printer 4 connected with the network is imparted on the

printing data automatically when the printer 4 prints the printing data in its self. Thereby it is easy to specify and trace the device and the location that performs the unauthorized copy of confidential documents in company or the forgery of bank notes and cash vouchers. Therefore, it is possible to prevent the spread of the leak of the secrecy information.

Besides, the copying device of the invention can be carried out by software of CPU and DSP. And it may be carried out by dedicated hardware, too.

In addition, the device can be installed as software of the secrecy document management into the database, the distribution system, the document change software like E-mail, or the document delivery software.

Since this embodiment of the invention can be applied to not only static images but also moving images, the invention adapts to the moving image data management.

Moreover, since the embodiment of the invention can accommodate to the various type of data, such as original image data, document text data, encrypted data and etc., in a scanner, a printer, and a personal computer, the invention can be utilized for not only the printing but also the monitor displaying.

As described above, it is possible to prevent the unauthorized copying and browsing of originals and electronic data in advance and speedy because the invention can update the copy inhibition information. Additionally, since the invention is provided with the secrecy management function, it is possible to stop the above inhibition function for a specific user corresponding to the secrecy management level granted to the user.

Furthermore, it is possible to trace the origin of the unauthorized copies since the information for identifying a device processing the printing

data can be added to the printing data.

Besides, each means described in each embodiment can be carried out by the configuration of hardware, and also can be carried out by a CPU and the programming installed in the CPU.

5

Possibility of Industrial Application

As described in the above embodiments, the invention can be adapted to the prevention of the unauthorized copying and browsing of documents and drawings in companies. Even in the same business office, 10 users who are allowed to copy and browse specific documents are distinguished from other users. In addition, the invention can be applied to the trace of a device that prepares copies of bank notes or cash vouchers which are inhibited to copy in general.

What is claimed is:

1. A data monitoring method comprising:

monitoring each copy element of monitoring object data consisting of at least one kind of copy element in accordance with at least one kind of copy inhibition information capable of being updated and stored in inhibition information storage; and

inhibiting input or output of the monitoring object data if the monitoring determines that said each copy element agrees with a kind of said copy inhibition information.

2. A data monitoring method according to claim 1, in which in the step of updating the copy inhibition information, the updating should be valid only when an authorized person executes the updating.

3. A data monitoring method according to claim 1, in which updating information of the copy inhibition information is provided by a removable storage media.

4. A data monitoring method according to claim 1, in which updating information of the copy inhibition information is provided by an information providing medium.

5. A data monitoring method according to claim 1, in which updating information of the copy inhibition information is provided passing through a network.

6. A data monitoring method according to claim 1, further

comprising:

storing updating logs when the copy inhibition information stored in the inhibition information storage is updated; and

in which in the step of updating copy inhibition information, the updating should be executed only when the updating information of the copy inhibition information is later than the stored log information.

7. A data monitoring method according to claim 1, further comprising:

10 controlling a copy inhibition or a inhibition cancel in accordance with secrecy management information and user's secrecy management level, said secrecy management information stored in the inhibition information storage in addition to the copy inhibition information in advance.

15 8. A data monitoring method according to claim 1, further comprising:

obtaining the copy inhibition information by requesting to a master information storage when originals of the copy inhibition information are stored in the master information storage on the network.

20

9. A data monitoring method according to claim 8, comprising:

controlling a copy inhibition or a inhibition cancel in accordance with secrecy management information and user's secrecy management level, said secrecy management information obtained together with the copy inhibition information at the step of obtaining the information, said secrecy management information stored in the master inhibition information storage in addition to the original copy inhibition information in advance.

25

10. A data monitoring method according to claim 1, comprising:
canceling a function of stopping the copying after confirming if a
user has a right to cancel the monitoring function or not.

5

11. A data monitoring device comprising:
an inhibition information storage storing at least one kind of copy
inhibition information that can be updated;

10 monitoring means monitoring at least one kind of copy element
prepared from monitoring object data based on the copy inhibition
information; and

inhibition means inhibiting input or output of the monitoring
object data if said at least one copy element included in the monitoring object
data agrees with one of the copy inhibition information.

15

12. A data monitoring device according to claim 11, further
comprising:

updating means updating the copy inhibition information.

20 13. A data monitoring device according to claim 12, in which the
updating means inhibits the updating when the updating is not executed by
a user having a right to update and the copy inhibition information has the
management information of the updating right as an attribute.

25 14. A data monitoring device according to claim 12, in which the
updating information is provided by a removable storage medium.

15. A data monitoring device according to claim 12, in which the updating information is obtained from an information providing medium.

16. A data monitoring device according to claim 15, in which the copy inhibition information is obtained passing through the network.

17. A data monitoring device according to claim 12, further comprising:

a log storage storing updating logs when the copy inhibition information in the inhibition information storage are updated; and

in which the updating means obtains the latest copy inhibition information based on the logs of the updating information.

18. A data monitoring device according to claim 12, further comprising:

secrecy management means storing in the inhibition information storage secrecy management information in addition to the copy inhibition information, and controlling a copy inhibition or a inhibition cancel in accordance with secrecy management information and user's secrecy management level.

19. A data monitoring device according to claim 12, further comprising:

a master information storage on the network storing originals of the copy inhibition information; and

information obtaining means obtaining the copy inhibition information by requesting to the master information storage.

20. A data monitoring device according to claim 19, in which the master storage stores secrecy management information of each original information in addition to the copy inhibition information;

5 the information obtaining means obtains the copy inhibition information and the secrecy management information; and further comprising:

10 secrecy management means controlling a copy inhibition or a inhibition cancel in accordance with the obtained secrecy management information and user's secrecy management level.

21. A data monitoring device according to claim 12, further comprising:

15 canceling means canceling a function of stopping the copying after confirming if a user has a right to cancel the monitoring function or not.

22. A copying device comprising:

20 first specific information extracting means extracting an ID information unique to a specific device concerned with the preparation of monitoring object data; and

information imparting means imparting the ID information to the monitoring object data and preparing a new copied data.

23. A copying device according to claim 22, in which the ID 25 information is chip ID information imparted to Central Processing Unit (CPU).

24. A copying device according to claim 22, in which the ID information is an IP address imparted to a device.

25. A copying device comprising:

5 second specific information extracting means extracting a specific application information unique to software concerned with the preparation of monitoring object data; and

information imparting means imparting the specific application information to the monitoring object data and preparing a new copied data.

10 26. A copying device according to claim 25, in which the specific application information is a mail address registered by a user.

15 27. A copying device receiving an monitoring object data from an external device and preparing a copy based on the monitoring object data, comprising:

extracting means analyzing the monitoring object data and extracting unique information specifying a specific device concerned with the preparation of the monitoring object data; and

20 specific information imparting means imparting the extracted unique information to the monitoring object data.

28. A copying device according to claim 27, in which the unique information is an ID number specifying a personal computer.

25 29. A copying device according to claim 27, in which the unique information is an IP address imparted to a device.

30. A copying device receiving an monitoring object data from an external device and preparing a copy based on the monitoring object data, comprising:

5 extracting means analyzing the copied data and extracting unique information specifying specific software concerned with the preparation of the copied data; and

specific information imparting means imparting the extracted unique information to the copied data as new copied data.

10

31. A copying device according to claim 30, in which the unique information is a mail address registered by a user.

15

32. A copying device according to claim 30, in which the unique information is registration information of software.

33. A copying device adapting to the network of receiving an monitoring object data from an external device and preparing a copy based on the monitoring object data, comprising:

20

extracting means extracting an IP address imparted to the copying device; and

specific information imparting means imparting the extracted IP address to the copied data as new copied data.

25

34. A storage medium storing programs comprising:

monitoring each copy element being monitoring object data consisting of at least one kind of copy element in accordance with at least one

kind of copy inhibition information capable of being updated and stored in inhibition information storage; and

inhibiting to input or output the monitoring object data if the monitoring determines that said each copy element agrees with a kind of
5 said copy inhibition information.

35. A storage medium storing a program comprising:

controlling a copy inhibition or a inhibition cancel in accordance with secrecy management information and user's secrecy management level,
10 said secrecy management information stored in the inhibition information storage in addition to the copy inhibition information in advance.

36. A storage medium executed by a copying apparatus preparing a copy according to monitoring object data after receiving the monitoring
15 object data from an external device or after preparing the monitoring object data by itself, which storing programs comprising:

extracting ID information unique to a specific device concerned with the preparation of the monitoring object data; and

imparting the ID information to the monitoring object data and
20 preparing a new copied data

37. A storage medium executed by a copying apparatus preparing a copy according to monitoring object data after receiving the monitoring
25 object data from an external device or after preparing the monitoring object data by itself, which storing programs comprising:

extracting specific application information unique to software concerned with the preparation of the monitoring object data; and

imparting the specific application information to the monitoring
object data and preparing a new copied data.

5

10

15

20

25

Abstract

Each copy elements of data being an object to be monitored such as printing data or reading data including at least one kind of copy elements is monitored according to at least one kind of copy inhibition information stored in inhibition information storage means and capable of being updated. By the monitoring, when one of the copy elements is judged to agree with the kind of coy inhibition information, input or output of the data being monitored is inhibited. Secrecy management information is given to the copy inhibition information, and a secrecy management level of a user is assigned to each user. In such a way, when the secrecy management level is higher than that of secrecy management information, the inhibition of the input or output is canceled. An ID for tracing a device which has copied a printed matter is given to the copied printed matter so as to prevent unauthorized copies form diffusing.

Fig. 1

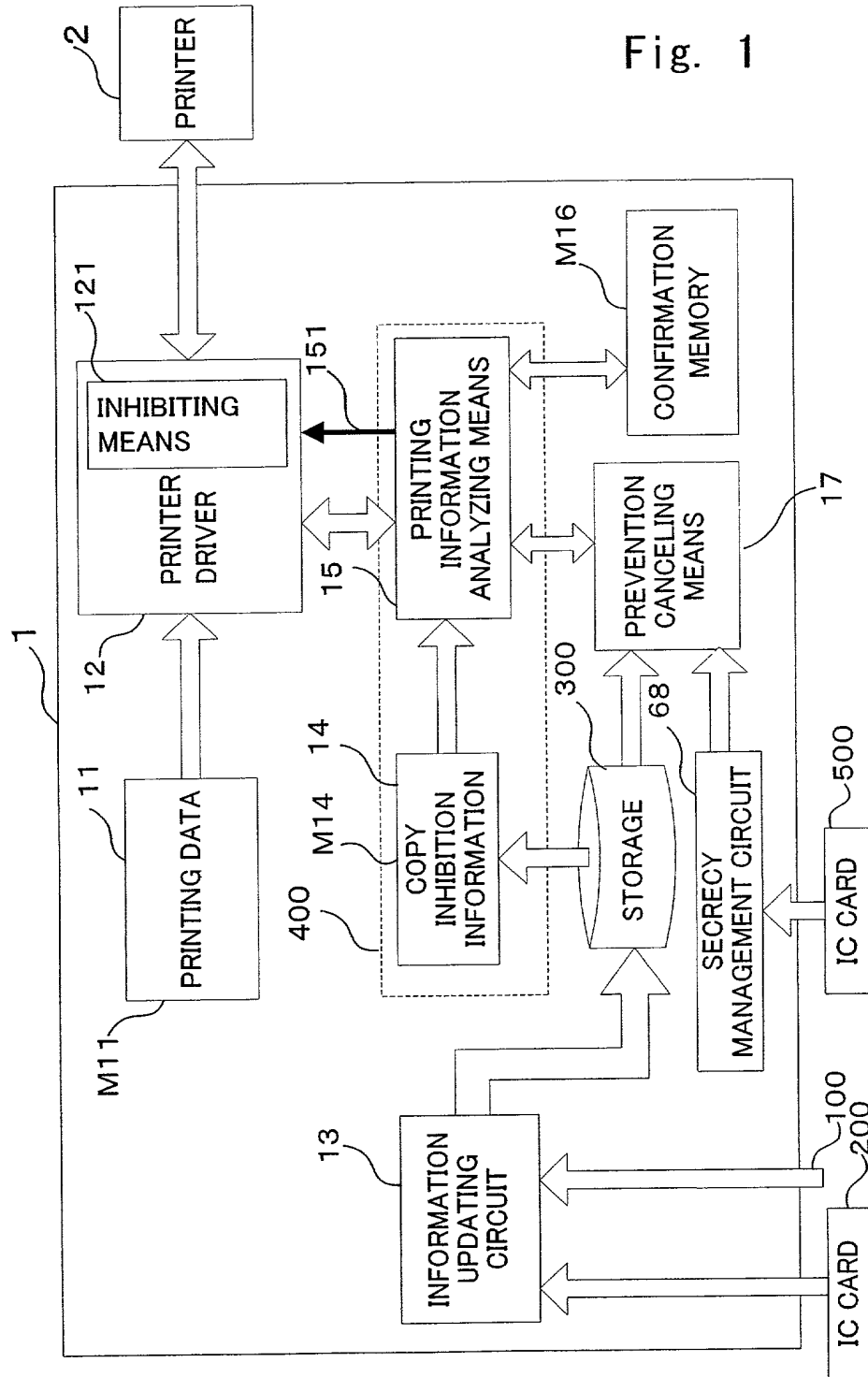
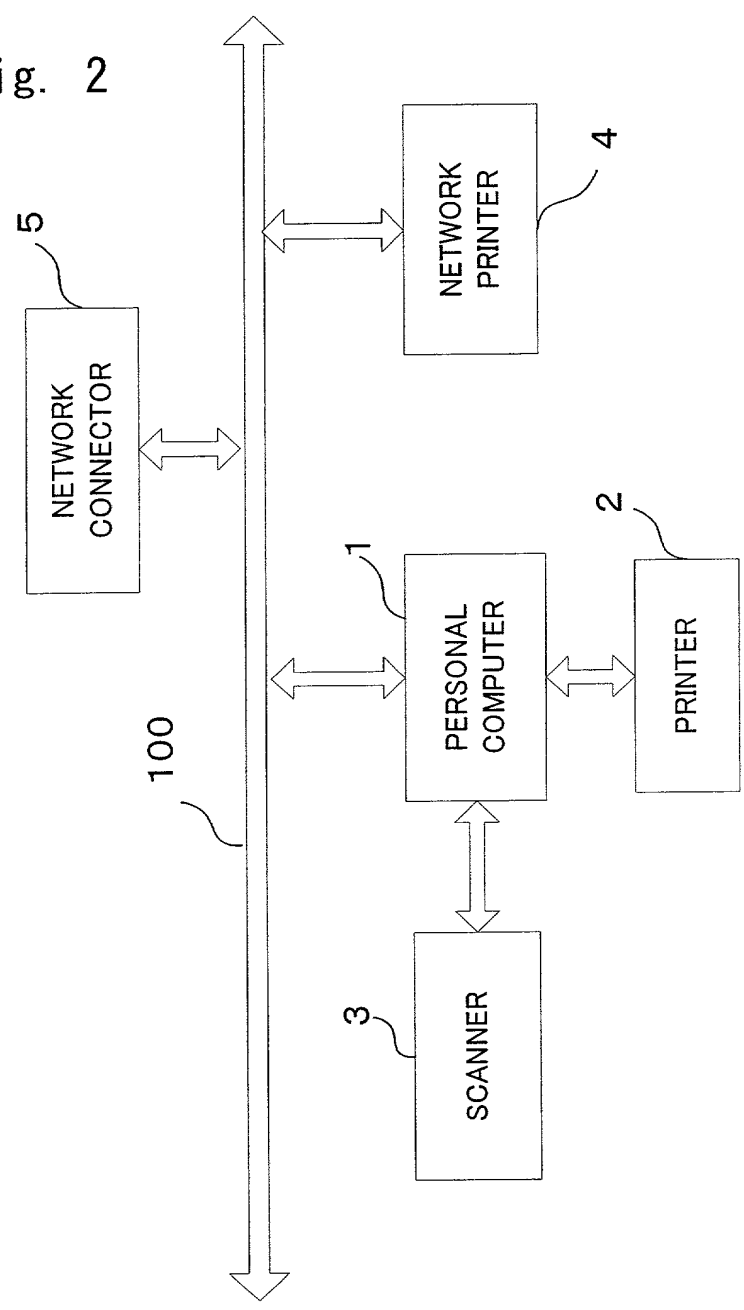


Fig. 2



3 / 18

Fig. 3

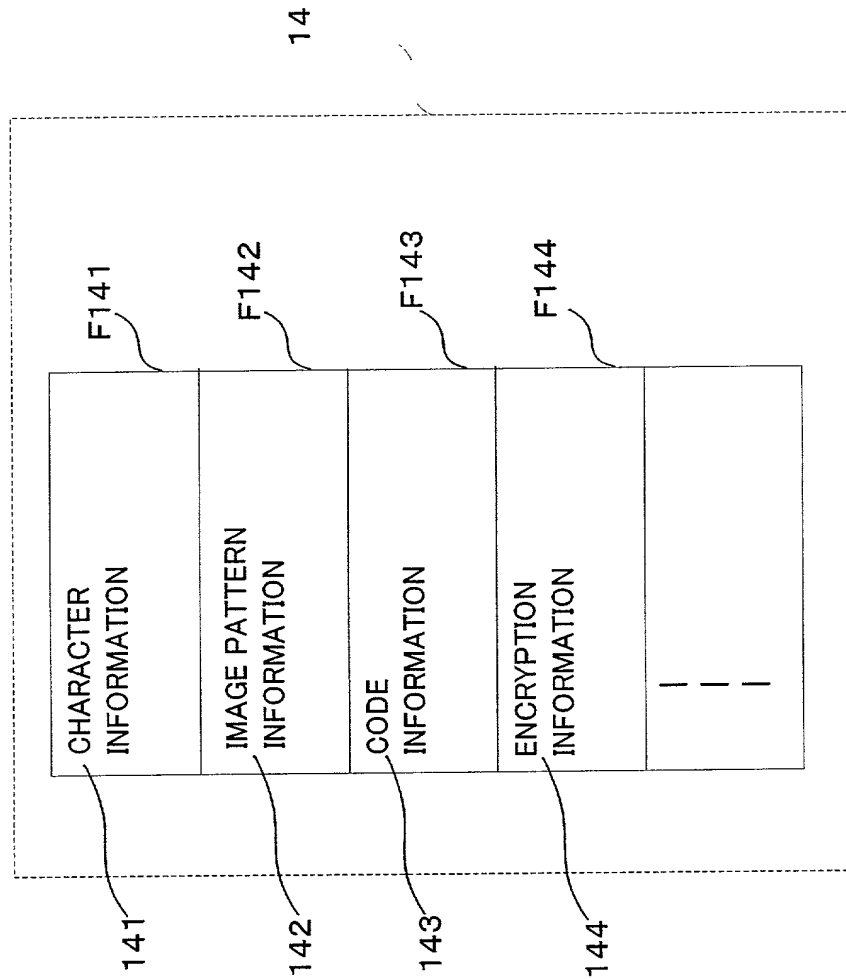


Fig. 4

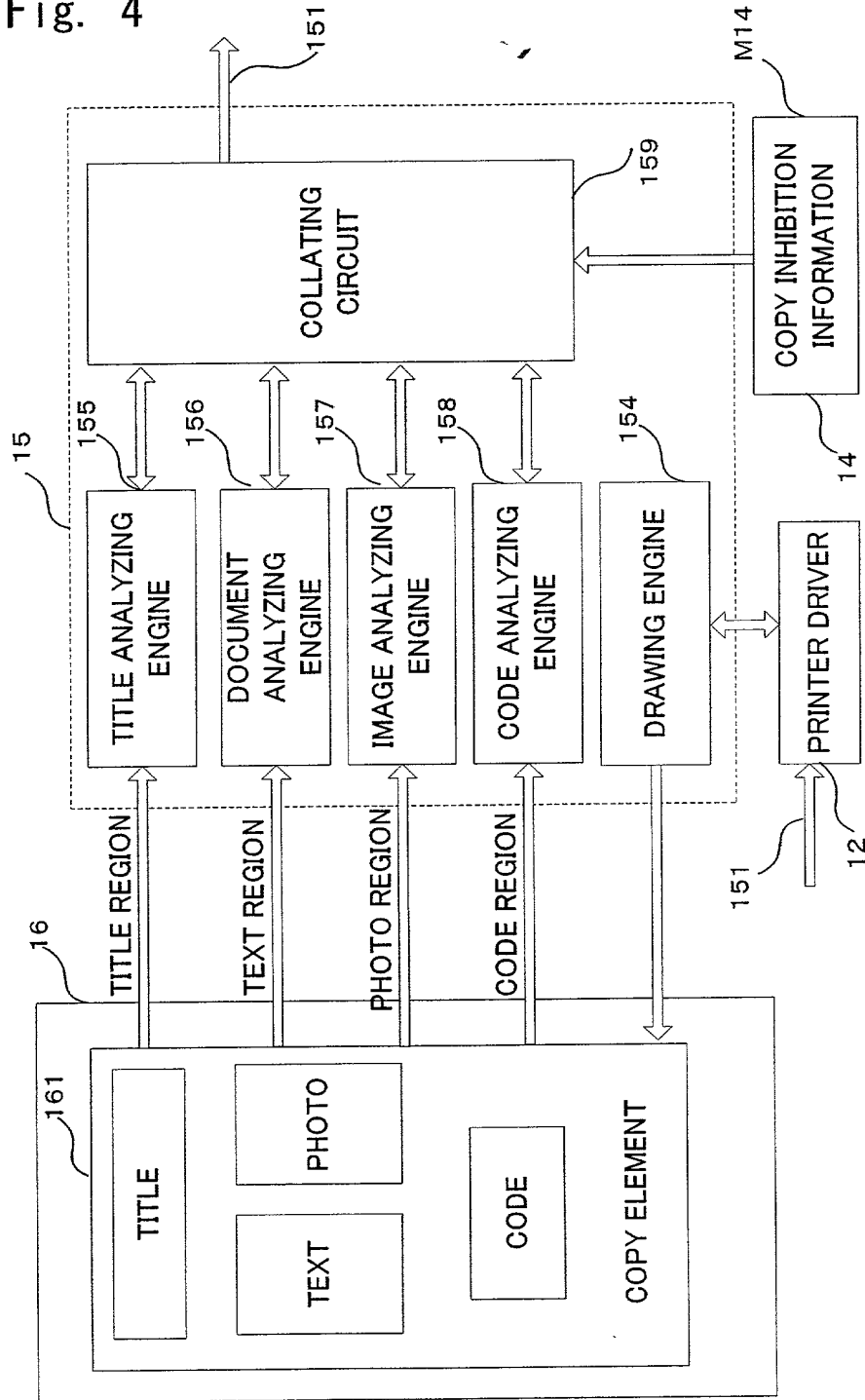


Fig. 5

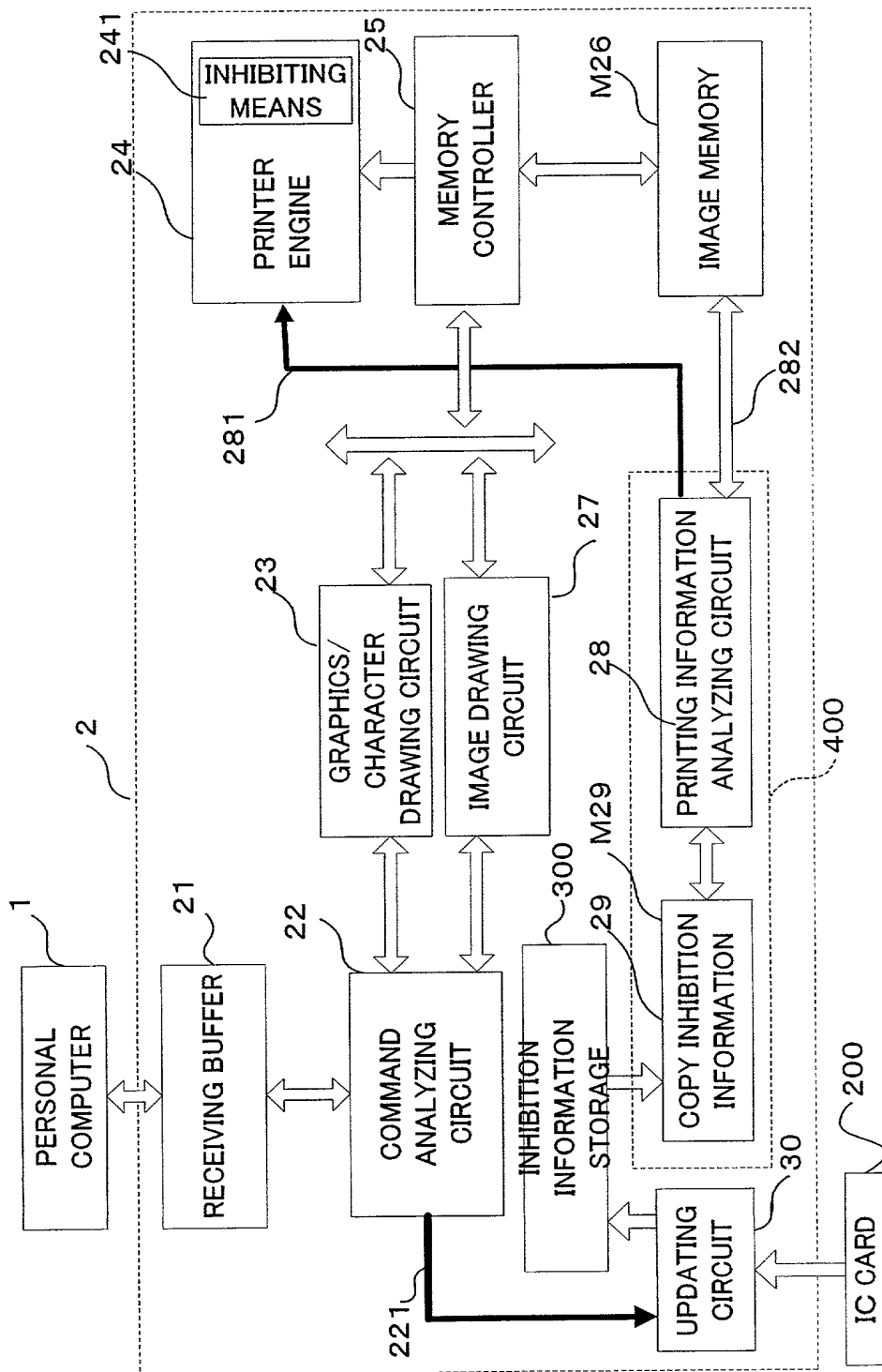


Fig. 6

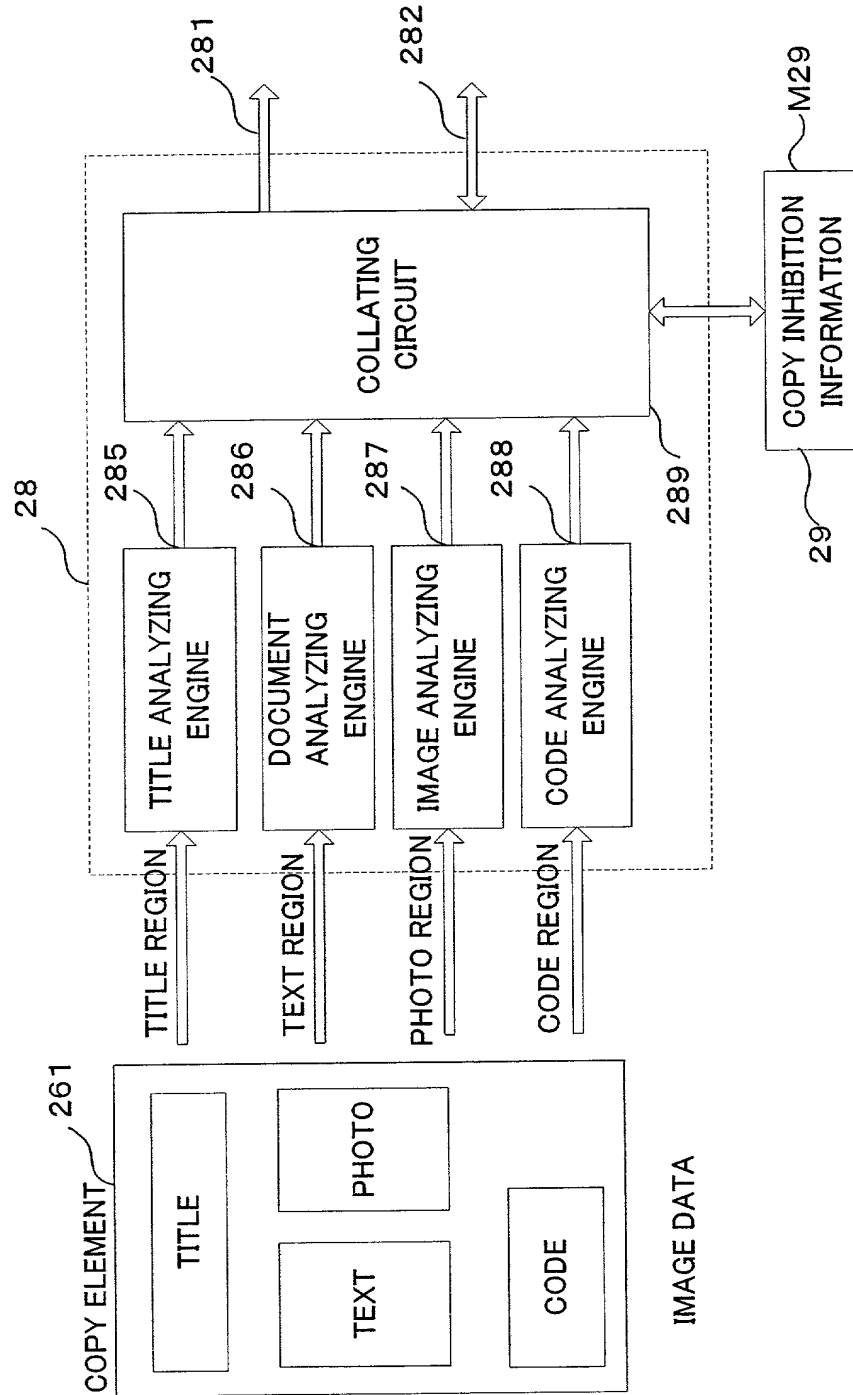


Fig. 7

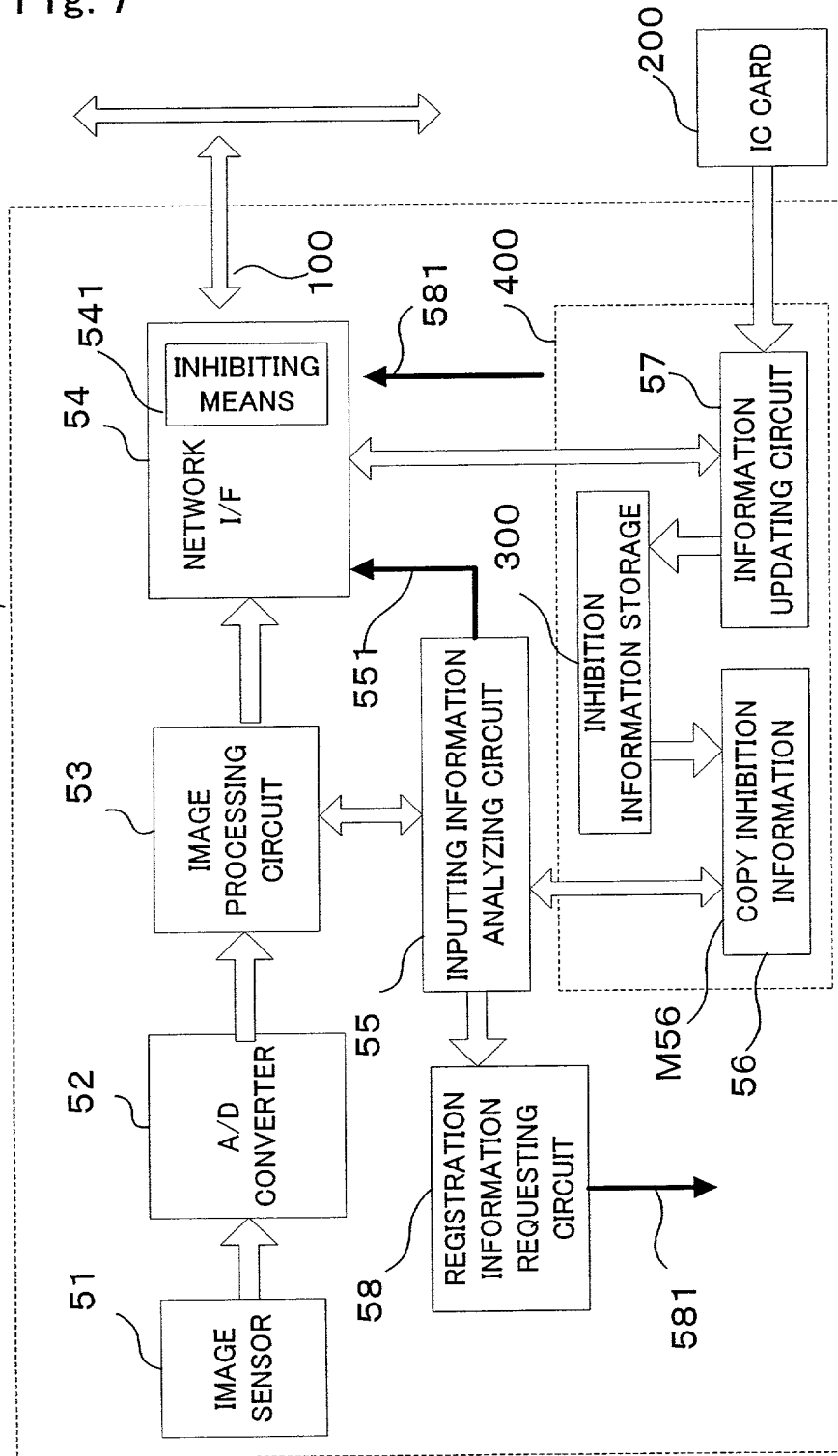


Fig. 8

8 / 18

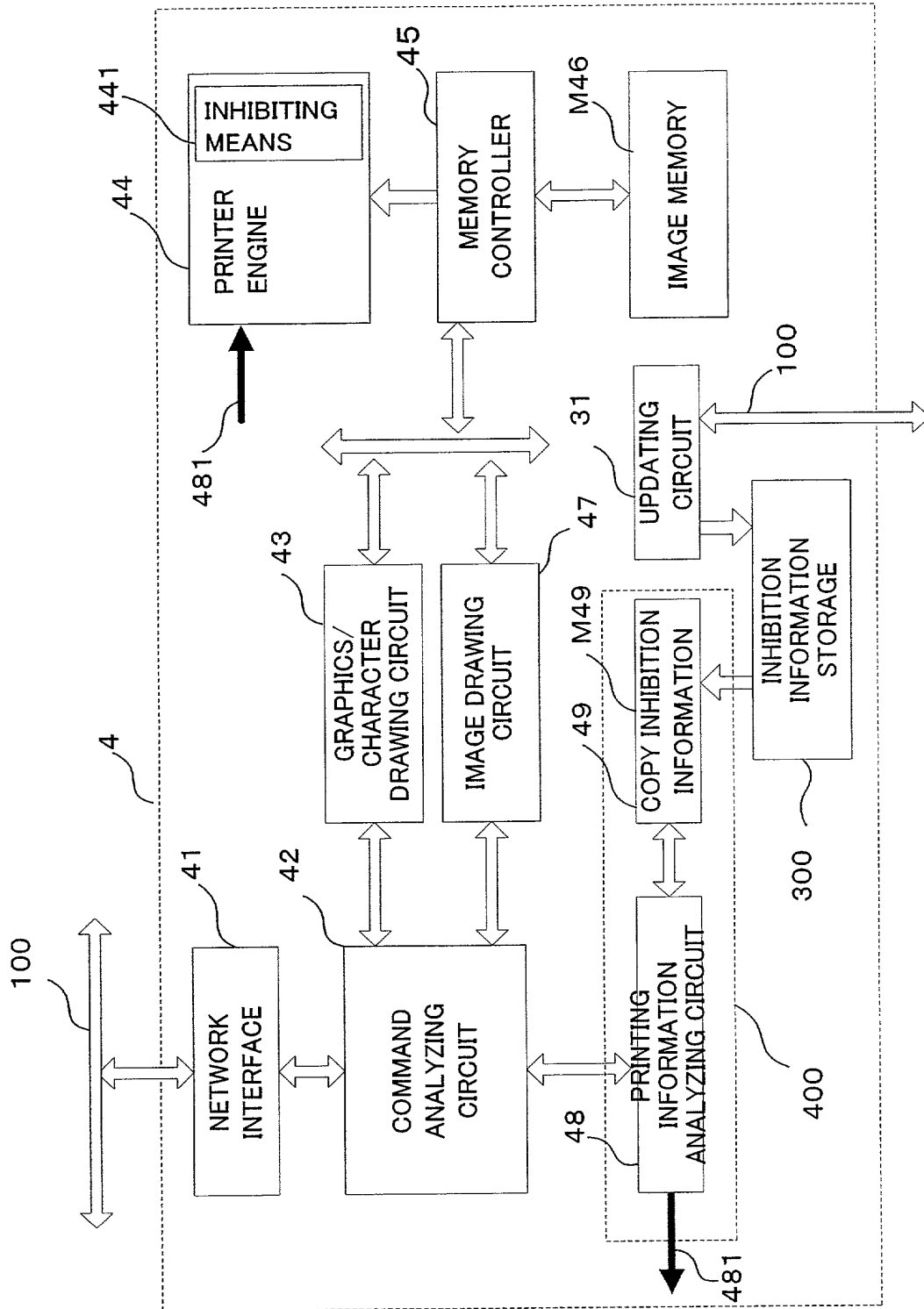


Fig. 9

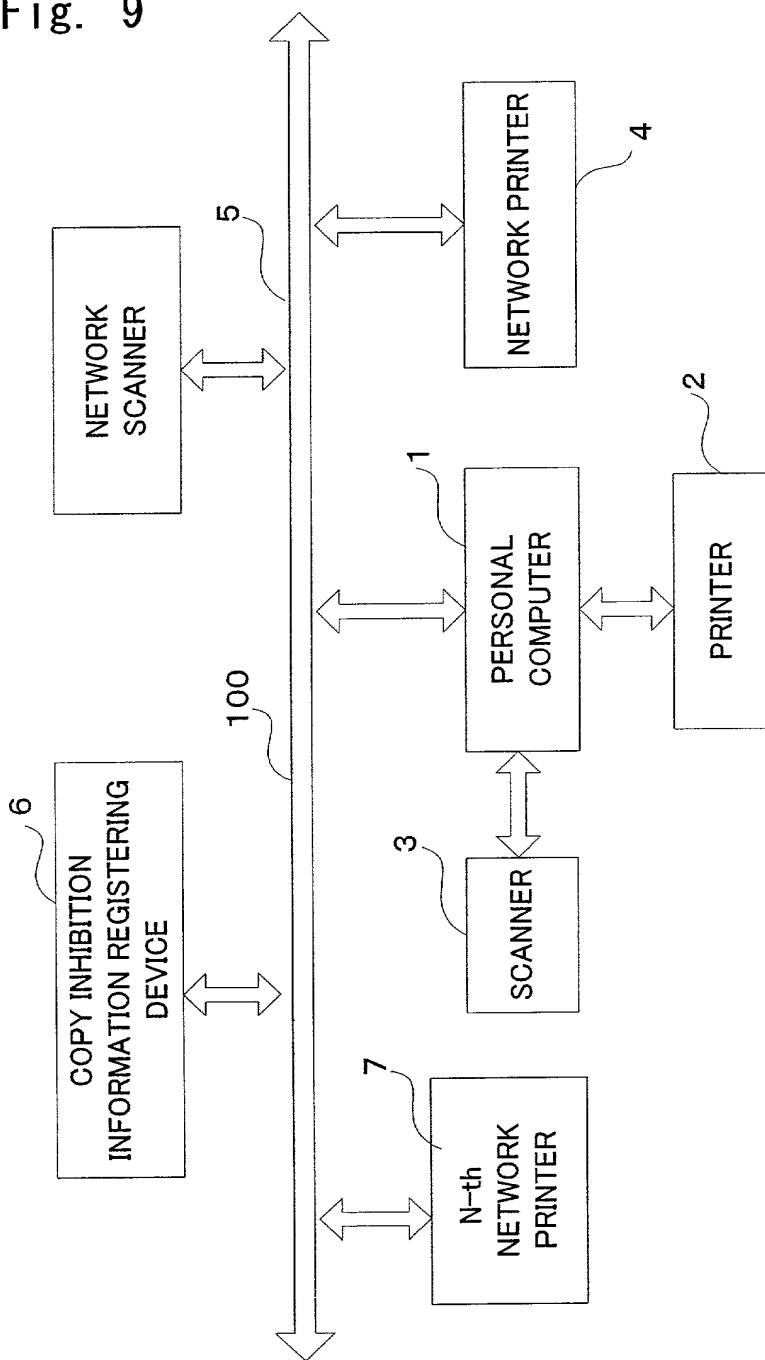


Fig. 10

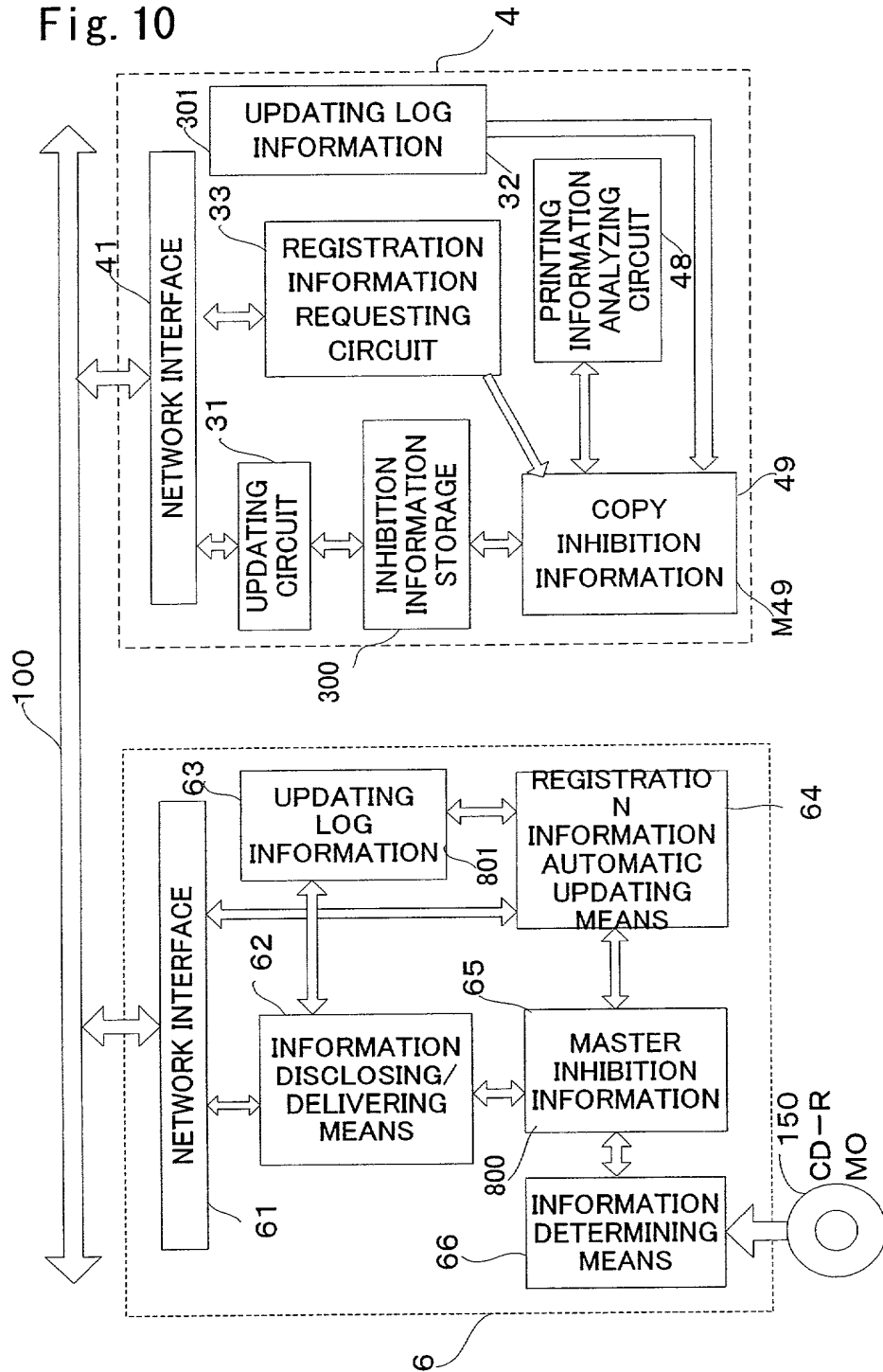


Fig. 11

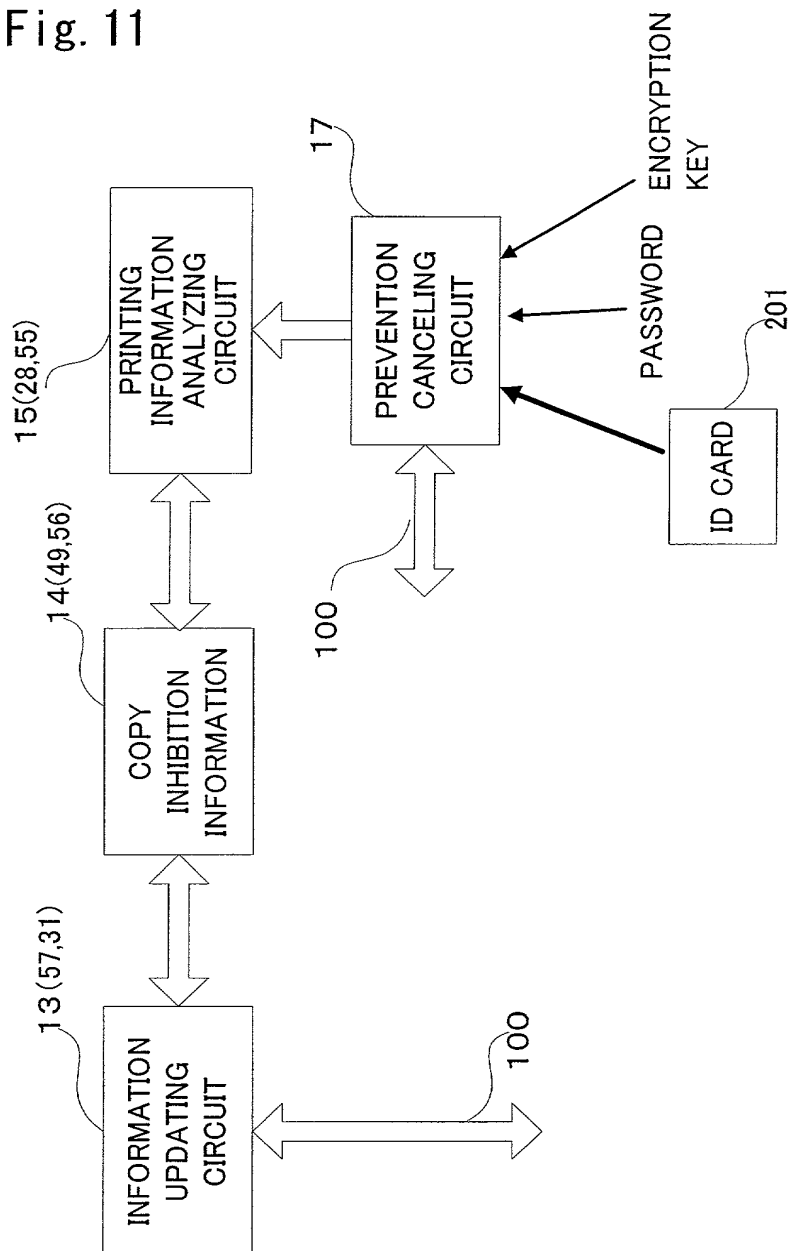


Fig. 12

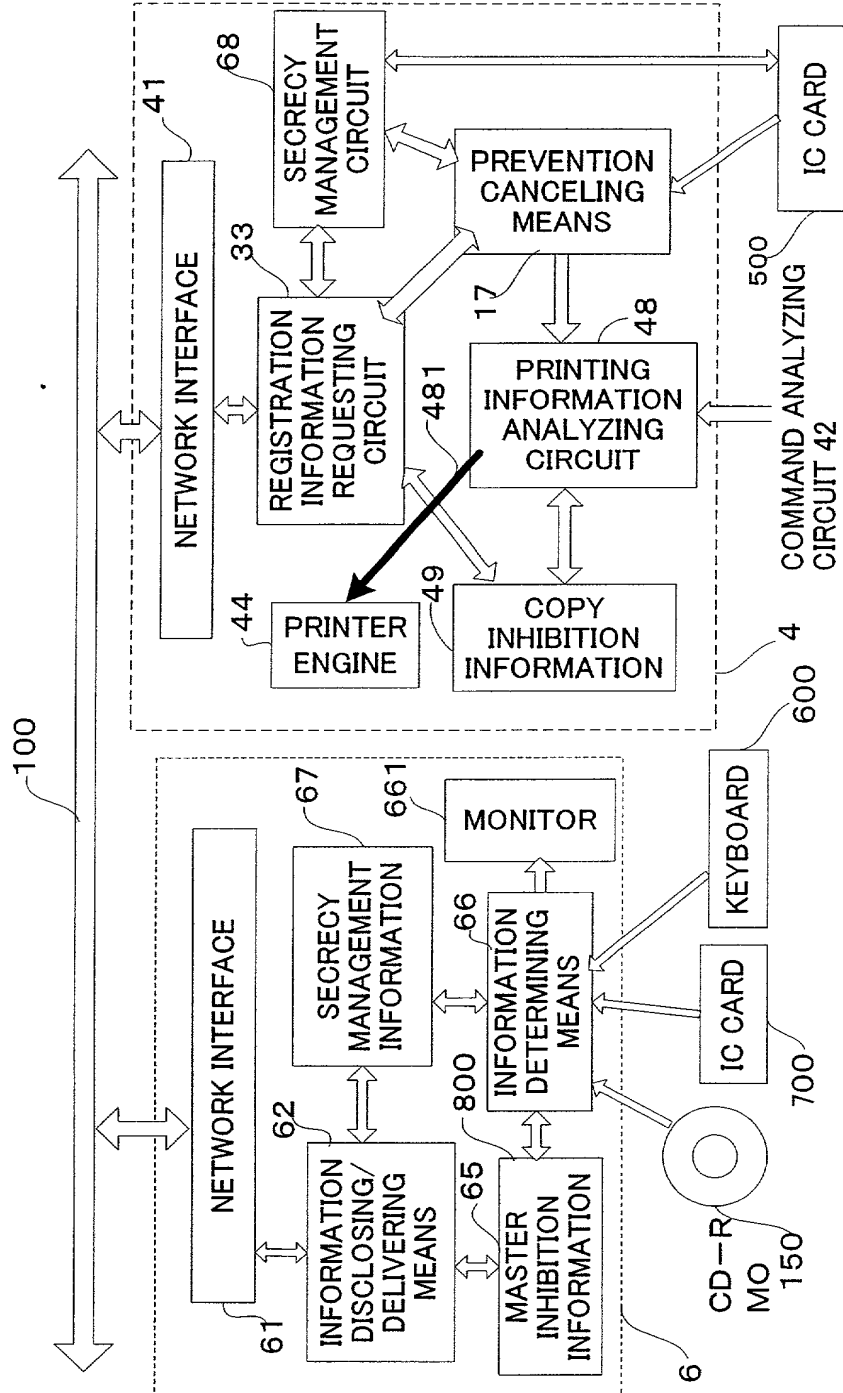


Fig. 13

670

INFORMATION ID	PERMIT LEVEL	GROUP ID	INDIVIDUAL ID
D001	A001	X00	ID1/PW1
D002	B001	X00	
D003	C001	X00	
D004	C002	Y00	ID1/PW1
D005	B002	Z00	
D006	A002	A00	ID1/PW1
⋮	⋮	⋮	⋮
Dnnn	P_lvl	Gnn	IDn/PWn

Fig. 14

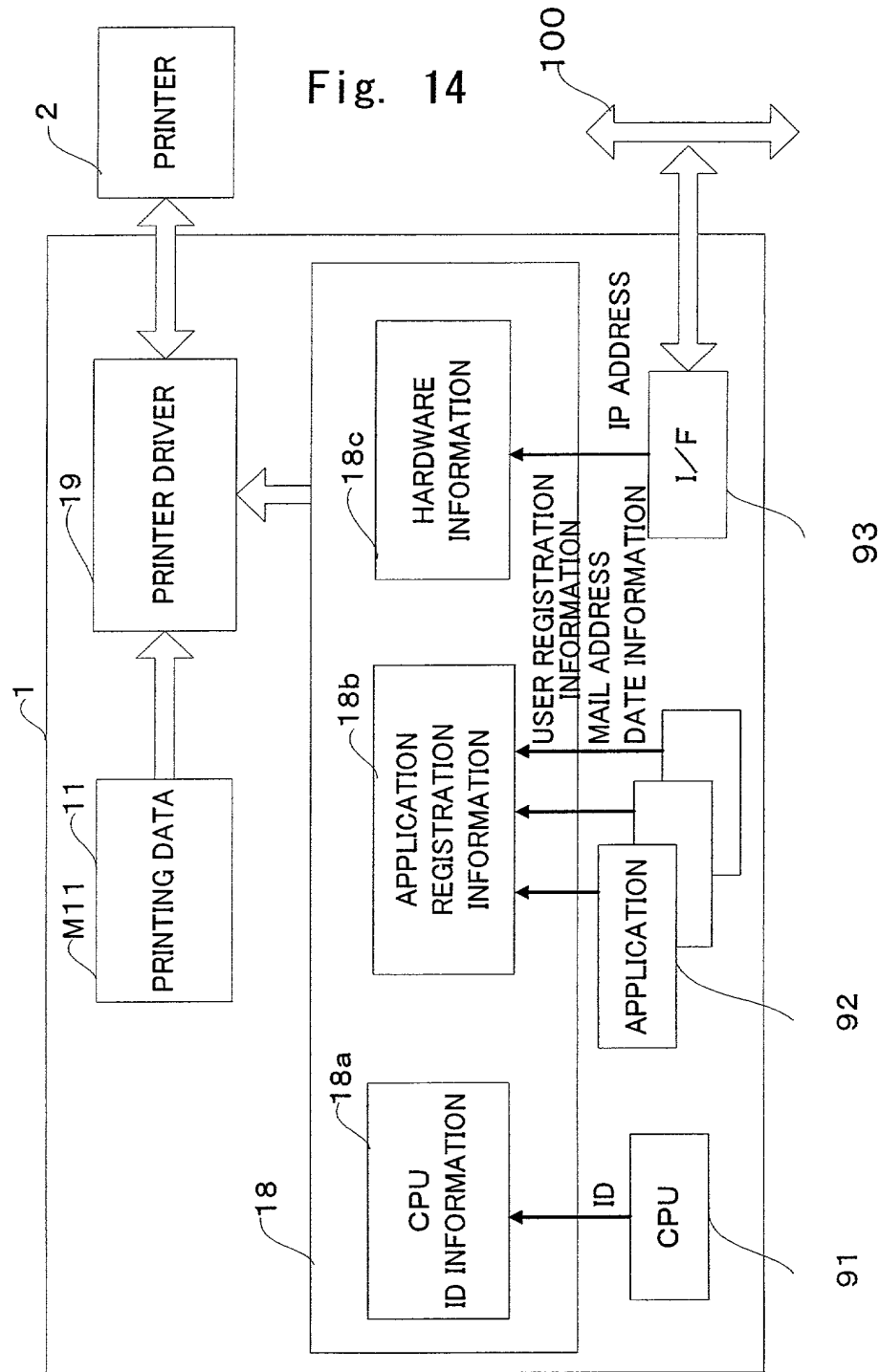


Fig. 15

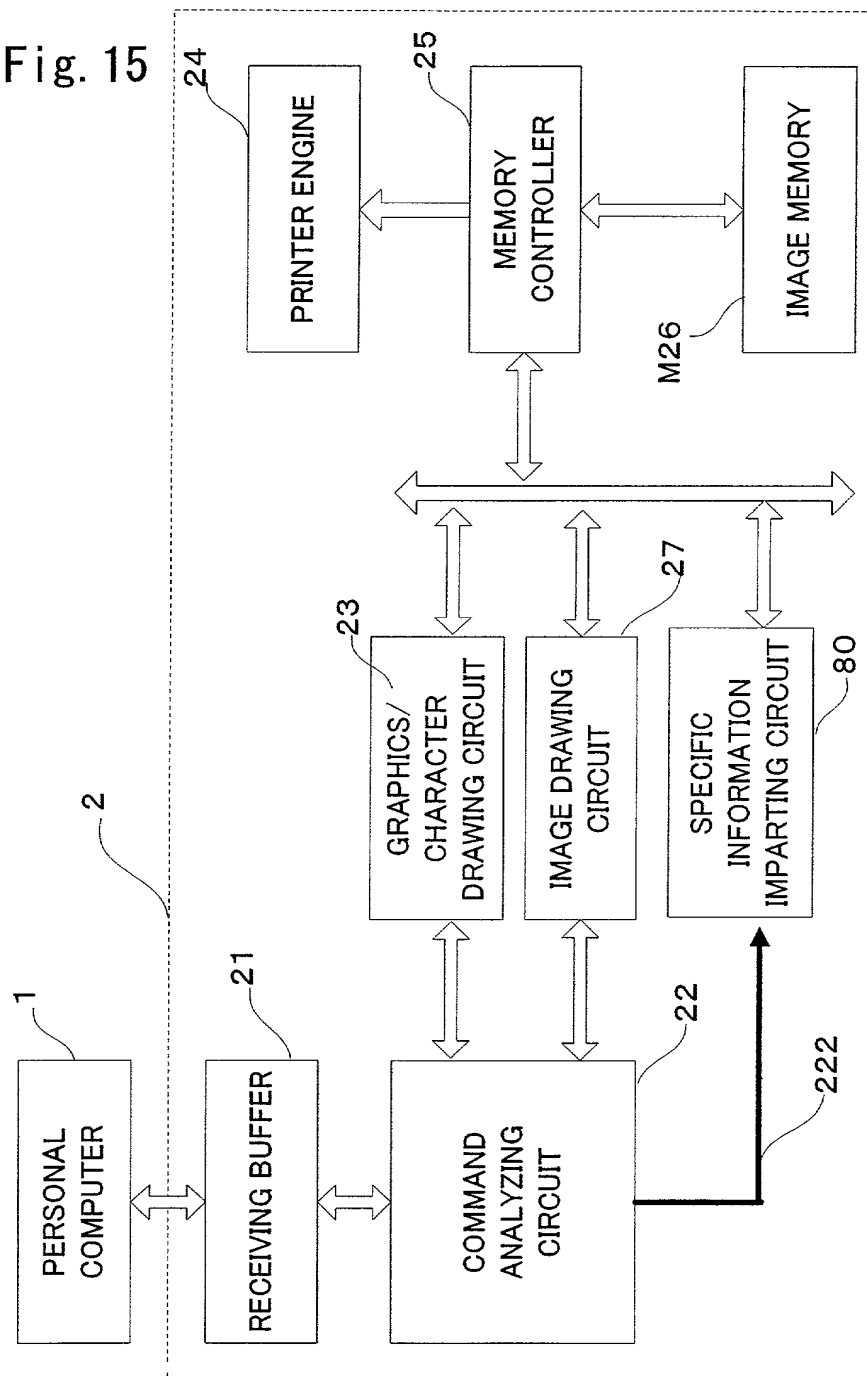


Fig. 16

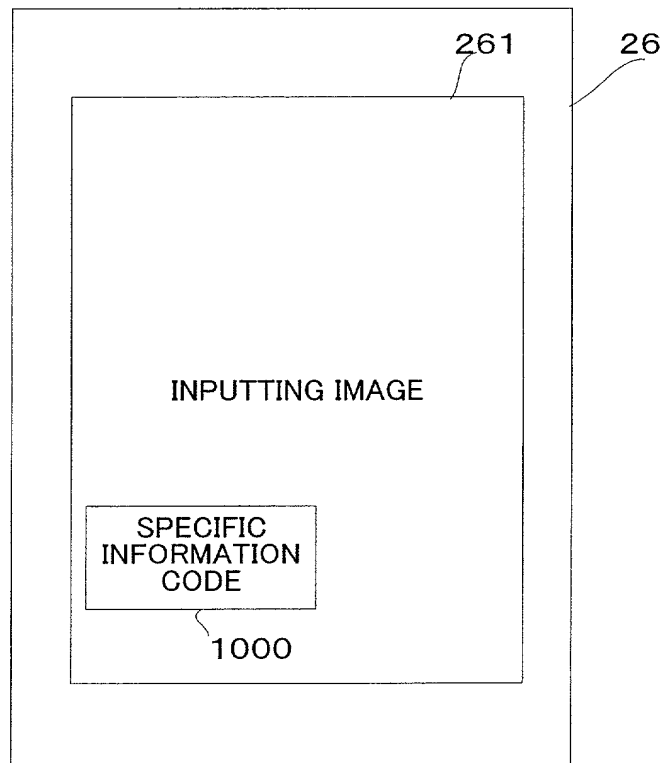


Fig. 17

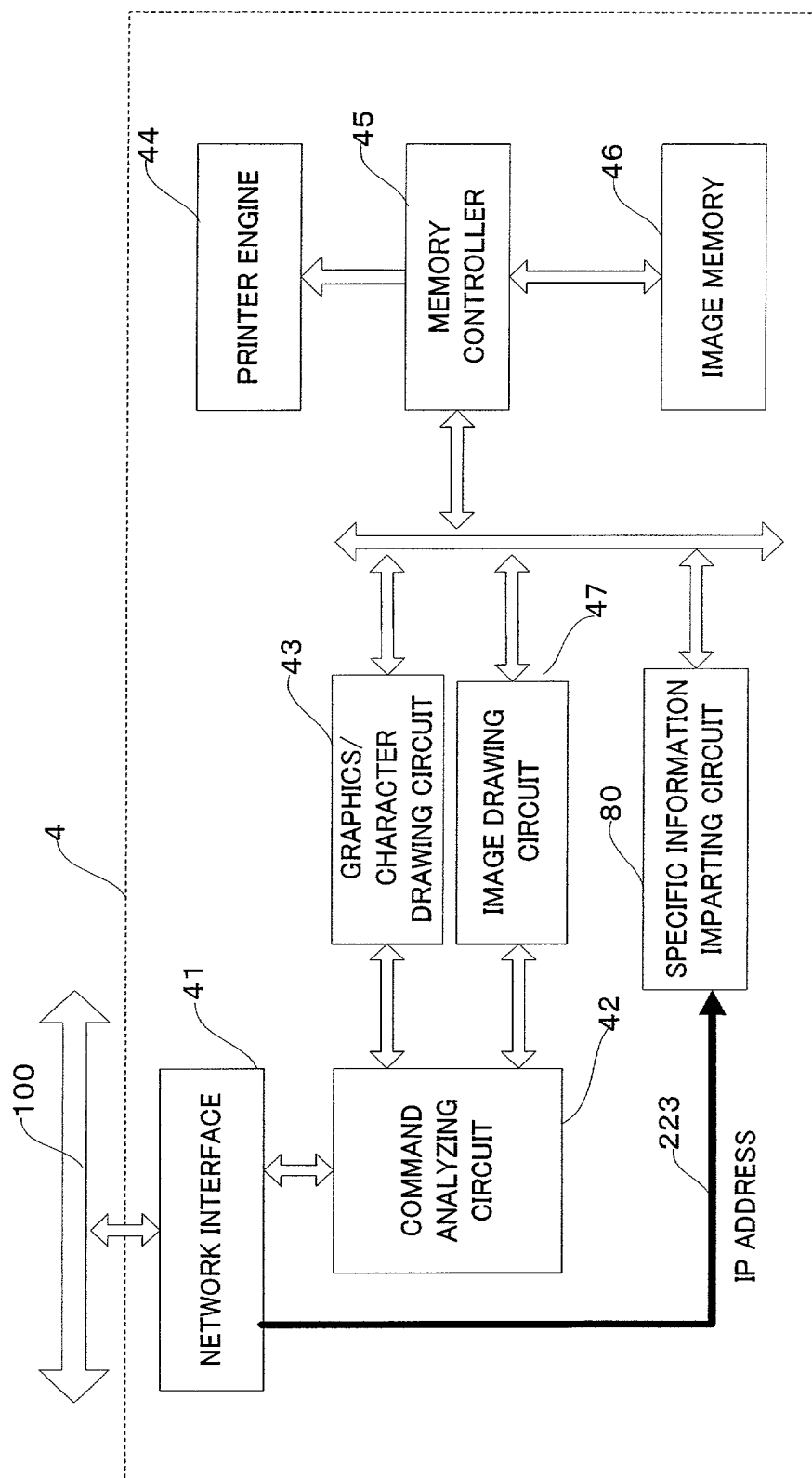
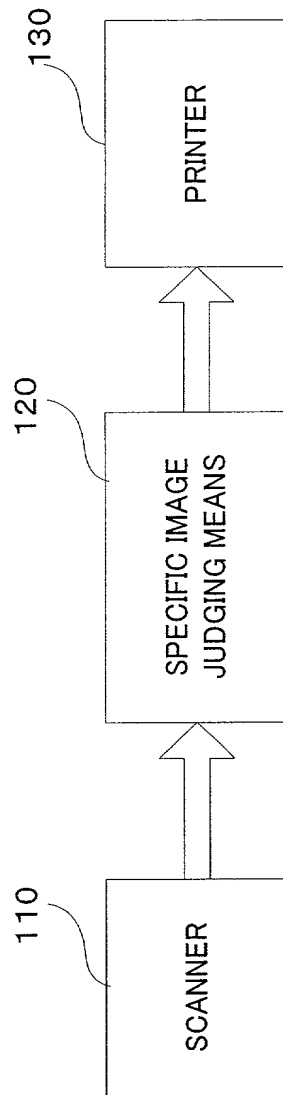


Fig. 18



COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

(Includes Reference to PCT International Application(s))

Attorney's Docket Number

(SAB)

As below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

DATA MONITORING METHOD, DATA MONITORING DEVICE, COPYING DEVICE, AND STORAGE MEDIUM

the specification of which:

- ☒ is attached hereto.
- ☐ was filed as United States application Serial No. _____
on _____
and was amended on _____ (if applicable).
- ☒ was filed as PCT international application Number PCT/JP00/01097
on February 25, 2000
and was amended under PCT Article 19 on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known to me to be material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or Section 365(b) of any foreign and/or international application(s) for patent or inventor's certificate or Section 365(a) of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY (If PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119
Japan	11-49996	February 26, 1999	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Japan	11-49997	February 26, 1999	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 USC §119(e) of any United States provisional application(s) listed below.

PRIOR PROVISIONAL APPLICATION(S):

Application Number	Filing Date

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s), or §365(c) of any PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application.

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. 120:

U.S. APPLICATIONS		STATUS (Check One)		
U.S. Application Number	U.S. Filing Date	Patented	Pending	Abandoned
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT Application No.	PCT Filing Date	U.S. Serial Numbers Assigned (if any)		
PCT/JP00/01097	February 25, 2000			

POWER OF ATTORNEY: As named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Stephen A. Becker, Reg. No. 26,527; John G. Bisbikis, Reg. No. 37,095; Christopher D. Bright, Reg. No. 46,578; Daniel Bucca, Reg. No. 42,368; Kenneth L. Cage, Reg. No. 26,151; Jennifer Chen, Reg. No. 42,404; Bernard P. Codd, Reg. No. 46,429; Lawrence T. Cullen, Reg. No. 44,489; Paul Devinsky, Reg. No. 28,553; Margaret M. Duncan, Reg. No. 30,879; Shamita De. Etienne-Cummings, Reg. No. 46,072; Ramyar M. Farid, Reg. No. 46,692; Brian E. Ferguson, Reg. No. 36,801; Michael E. Fogarty, Reg. No. 36,139; John R. Fuisz, Reg. No. 37,327; Willem F. Gadiano, Reg. No. 37,136; Keith E. George, Reg. No. 34,111; Matthew V. Grumbling, Reg. No. 44,427; John A. Hankins, Reg. No. 32,029; Eric J. Kraus, Reg. No. 36,190; Catherine Krupka, Reg. No. 46,227; Jack Q. Lever, Reg. No. 28,149; Raphael V. Lupo, Reg. No. 28,363; Burman Y. Mathis III, Reg. No. 44,902; Michael A. Messina, Reg. No. 33,424; Dawn L. Palmer, Reg. No. 41,238; Joseph H. Paquin, Jr., Reg. No. 31,647; Scott D. Paul, Reg. No. 42,984; William D. Pegg, Reg. No. 42,988; Robert L. Price, Reg. No. 22,685; Gene Z. Robinson, Reg. No. 33,351; Mahshid D. Saadat, Reg. No. P-48,218; Joy Ann G. Serauskas, Reg. No. 27,952; Daniel H. Sherr, Reg. No. 46,425; David A. Spenard, Reg. No. 37,449; Arthur J. Steiner, Reg. No. 26,106; David L. Stewart, Reg. No. 37,578; Wesley Strickland, Reg. No. 44,363; Michael D. Switzer, Reg. No. 39,552; Daniel S. Trainor, Reg. No. 43,959; Cameron K. Weiffenbach, Reg. No. 44,488; Aaron Weisstuch, Reg. No. 41,557; Edward J. Wise, Reg. No. 34,523; Jeffrey A. Woller, Reg. No. 48,041; Alexander V. Yampolsky, Reg. No. 36,324; and Robert W. Zelnick, Reg. No. 36,976, all of McDermott, Will & Emery.

Send Correspondence to:	Direct Telephone Calls to: (name and telephone number)
McDERMOTT, WILL & EMERY 600 13 th Street, N.W. Washington, D.C. 20005-3096	(202) 756-8000

	Full Name of Inventor	Family Name	First Given Name	Second Given Name
201	Akio KOJIMA	KOJIMA	Akio	
	Residence and Citizenship	City	State or Foreign Country	Country of Citizenship
	Neyagawa	Neyagawa-shi	Osaka	JAPAN
	Post Office Address	Post Office Address	City	State & Zip Code/Country
	3-9-7-205	Ikeda	Neyagawa-shi	Osaka 572-0039 JAPAN
202	Yasuhiro KUWAHARA	KUWAHARA	Yasuhiro	
	Residence and Citizenship	City	State or Foreign Country	Country of Citizenship
	Moriguchi	Moriguchi-shi	Osaka	JAPAN
	Post Office Address	Post Office Address	City	State & Zip Code/Country
	3-32-11-603	Dainichi-cho	Moriguchi-shi	Osaka 570-0003 JAPAN

